高职高专计算机任务驱动模式教材

计算机网络基础

满昌勇 主编
崔学鹏 赵文正 副主编



清华大学出版社

高职高专计算机任务驱动模式教材

计算机网络基础

满昌勇　主　编
崔学鹏　赵文正　副主编

清华大学出版社
北　京

内 容 简 介

全书共分 8 个模块，主要内容包括认识计算机网络、网络数据通信基础、网络体系结构与协议、组建局域网、互联网的使用、网络的管理、网络管理与网络安全以及案例分析——校园网的建设。

本书面向的是计算机网络的初学者，读者只要具备基本的计算机文化基础知识就可以随着本书的任务指导，掌握相关知识与应用。同时，本书将任务驱动与理论学习相结合，由浅入深，循序渐进，也适合大中专院校的教师将其作为授课教材。

图书在版编目（CIP）数据

计算机网络基础/满昌勇主编. --北京：清华大学出版社，2010.1
（高职高专计算机任务驱动模式教材）
ISBN 978-7-302-21683-4

Ⅰ. ①计… Ⅱ. ①满… Ⅲ. ①计算机网络—高等学校：技术学校—教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2009）第 238570 号

责任编辑：束传政 张龙卿
责任校对：刘 静
责任印制：

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　　**印　张**：17　　**字　　数**：386 千字
版　　次：2010 年 1 月第 1 版　　**印　　次**：2010 年 1 月第1 次印刷
印　　数：1～ 000
定　　价： .00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：030019-01

编审委员会

出版说明

我国高职高专教育经过近10年的发展，已经转向深度教学改革阶段。教育部2006年12月发布了教高[2006]16号文件“关于全面提高高等职业教育教学质量的若干意见”，大力推行工学结合，突出实践能力培养，全面提高高职高专教学质量。

清华大学出版社作为国内大学出版社的领跑者，为了进一步推动高职高专计算机专业教材的建设工作，适应高职高专院校计算机类人才培养的发展趋势，根据教高[2006]16号文件的精神，2007年秋季开始了新一轮教学改革的教材建设工作。

目前国内高职高专院校计算机网络与软件专业的教材品种繁多，但切合国家计算机网络与软件技术专业领域技能型紧缺人才培养培训方案并符合企业的实际需要，能够成体系的教材还不成熟。

我们组织国内对计算机网络和软件人才培养模式有研究并且有实践经验的高职高专院校，进行了较长时间的研讨和调研，遴选出一批富有工程实践经验和教学经验的双师型教师，合力编写了这套适用于高职高专计算机网络、软件专业的教材。

本套教材的编写方法是以任务驱动案例教学为核心，以项目开发为主线。我们研究分析了国内外先进职业教育的培训模式、教学方法和教材特色，消化吸收优秀的经验和成果。以培养技术应用型人才为目标，以企业对人才的需要为依据，把软件工程和项目管理的思想完全融入教材体系，将基本技能培养和主流技术相结合，课程设置中重点突出、主辅分明、结构合理、衔接紧凑。教材侧重培养学生的实战操作能力，学、思、练相结合，旨在通过项目实践，增强学生的职业能力，使知识从书本中释放并转化为专业技能。

一、教材编写思想

本套教材以案例为中心，以技能培养为目标，围绕开发项目所用到的知识点进行讲解，对某些知识点附上相关的例题，以帮助读者理解，进而将知识转变为技能。

考虑到是以“项目设计”为核心组织教学，所以在每一学期配有相应的

实训课程及项目开发手册，要求学生在教师的指导下，能整合本学期所学的知识内容，相互协作，综合应用该学期的知识进行项目开发。同时在教材中采用了大量的案例，这些案例紧密地结合教材中的各个知识点，循序渐进，由浅入深，在整体上体现了内容主导、实例解析、以点带面的模式，以配合课程后期以“项目设计”贯穿教学内容的教学模式。

软件开发技术具有种类繁多、更新速度快的特点。本套教材在介绍软件开发主流技术的同时，帮助学生建立软件相关技术的横向及纵向的关系，培养学生综合应用所学知识的能力。

二、丛书特色

本系列教材体现目前的工学结合教改思想，充分结合教改现状，突出项目面向教学和任务驱动模式教学改革成果，打造立体化精品教材。

(1) 参照和吸纳国内外优秀计算机网络、软件专业教材的编写思想，采用本土化的实际项目或者任务，以保证其有更强的实用性，并与理论内容有很强的关联性。

(2) 准确把握高职高专软件专业人才的培养目标和特点。

(3) 充分调查研究国内软件企业，确定了基于 Java 和.NET 的两个主流技术路线，再将其组合成相应的课程链。

(4) 教材通过一个个的教学任务或者教学项目，在做中学，在学中做，以及边学边做，重点突出技能培养。在突出技能培养的同时，还介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

(5) 借鉴或采用项目驱动的教学方法和考核制度，突出计算机网络、软件人才培训的先进性、工具性、实践性和应用性。

(6) 以案例为中心，以能力培养为目标，并以实际工作的例子引入概念，符合学生的认知规律。语言简洁明了、清晰易懂，更具人性化。

(7) 符合国家计算机网络、软件人才的培养目标；采用引入知识点、讲述知识点、强化知识点、应用知识点、综合知识点的模式，由浅入深地展开对技术内容的讲述。

(8) 为了便于教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务资源。在清华大学出版社网站(www.tup.com.cn)免费提供教材的电子课件、案例库等资源。

高职高专教育正处于新一轮教学深度改革时期，从专业设置、课程体系建设到教材建设，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并及时反馈给我们。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育继续出版优秀的高质量的教材。

清华大学出版社

高职高专计算机专业教材编审委员会

rawstone@126.com

前　言

随着教育改革的不断深入，高等职业教育技术进入到一个迅速发展的历史阶段。计算机网络是当今计算机科学与技术学科中发展最为迅速的技术之一，也是计算机应用中最为普及和活跃的领域。可以预见，计算机网络的发展需要大量具有系统知识与实际技能的专门人才。本书作者在多年的教学中体会到现有的网络技术教材多数重理论轻实践，以学历教育的思想对待高等职业教育已不能适应培养专业技术人才的需要。随着教育改革的深入，任务驱动教学法在高等职业教育领域得到广泛的认可与应用。对于专业基础课，同样可以使用任务驱动的方式把知识与实际应用相结合，使教学与学习都有的放矢。基于此，本书作者以极大的热情和希望投入到本书的编写中。

本书以计算机网络基础知识为主线，以模块化任务为驱动，遵循优化结构、精选内容的原则。全书共分 8 个模块。

模块 1 介绍认识计算机网络。通过两个任务引入网络的定义、结构与功能。

模块 2 介绍网络数据通信基础。以制作网线、利用示波器查看信号等任务，学习数据传输、传输介质、数据编码、数据交换与差错控制等知识。

模块 3 介绍网络体系结构与协议。通过计算机 MAC 地址的寻找，介绍网络体系结构与协议的相关知识。

模块 4 介绍组建局域网。通过组建局域网与无限局域网介绍局域网的工作原理与组成。

模块 5 介绍互联网的使用。通过配置计算机联网、使用 FTP 上传与下载、组建家庭网络等任务，介绍互联网的接入与应用等相关知识。

模块 6 介绍网络的管理。通过完成 Windows Server 2003 的安装与配置、IIS 的安装与 Web 站点发布等任务，介绍网络管理的相关知识。

模块 7 介绍网络管理与网络安全。通过使用金山杀毒软件，了解网络安全威胁与对策等知识；通过解决计算机无法登录服务器等问题，介绍网络常见故障及其解决办法。

模块 8 介绍案例分析——校园网的建设。分析校园网建设的实际案例，介绍项目开发的过程，贯通全书所学。

本书编写分工如下：满昌勇老师编写了模块1、模块6，并参与了模块3、模块4、模块5、模块7部分内容的编写；崔学鹏老师编写了模块3、模块4和模块8；赵文正老师编写了模块5和模块8的部分内容；王永杰老师参与了模块6和模块7的编写；金永亮老师负责模块2的编写；王永斌老师参与了模块4和模块5的编写；孙连军老师认真严格的审稿保证了本书的质量。另外，在本书的编写过程中，得到了清华大学出版社的大力协助与支持，在此一并表示衷心的感谢。

教学建议：建议用一学期完成本课程教学，90学时左右，其中实训学时不低于三分之一；教学过程中用任务引导知识的讲解，结合相应实训过程提高教学效果；任课老师可根据情况需要，对任务进行细化分解，也可对内容进行取舍。

由于编者时间、能力有限，加之计算机网络技术日新月异，书中难免有不妥和疏漏之处，恳请广大读者批评指正。

编　者

2009年10月

目　录

模块 1　认识计算机网络

任务 1.1　认识计算机网络

任务描述：某实验室有 20 台个人计算机，1 台文件服务器，1 台共享打印机，在文件服务器上安装了常用软件并且有这些软件的备份。如果要求个人计算机能够使用这些软件，并且能够利用打印机，这些设备应该如何连接？

1.1.1　什么是计算机网络

按照任务要求，需要完成计算机的连接，共享计算机的软硬件资源，这涉及计算机网络的问题。本节首先要解决的问题：什么是计算机网络？

对于计算机网络，多年来并没有一个严格的定义。随着网络的发展，计算机网络具有不同的内涵。网络的定义大致可以分为三类：资源共享的观点、广义的观点与用户透明性的观点。

1. 资源共享的观点

资源共享的观点将计算机网络定义为“以能够相互共享资源的方式互联起来的自治的计算机系统的集合”。这种定义比较准确地描述了计算机网络的基本特征。

(1) 群体性问题，计算机网络是计算机系统的集合，是一种多机系统。

(2) 独立性问题，网络上的计算机是“自治计算机”，也就是说计算机网络系统中的计算机(也称为工作站)具有独立性。如果其中某台计算机可以被其他计算机强制控制，则不能满足独立性的原则，不能构成计算机网络系统。

(3) 互联性问题，网络互联既包括物理上的连接，也包括软件连接，完成互联需要有网络协议和网络操作系统的支持。

(4) 计算机网络系统的主要目的是资源共享(包括硬件、软件、数据等)。通过将物理上分散的若干计算机有机连接起来，达到资源共享和协同工作等目标的系统。

2. 广义的观点

广义的观点将计算机网络定义为“计算机技术与通信技术相结合，实现远程信息处理从而进一步达到资源共享的系统”。计算机网络发展到“计算机—计算机”之间的连接阶段，又提出了计算机通信网的定义：“在计算机间以传输信息为目的连接起来的计算机系统的集合。”

3. 用户透明性的观点

从用户透明性的观点出发，定义计算机网络为“存在着一个能为用户自动管理资源的网络操作系统，由它调用完成用户任务所需要的资源，而整个网络像一个大的计算机系统一样对用户是透明的”。严格来讲，用户透明性观点的定义所论述的是一种分布式计算机

系统。分布式系统实际上就是建立在计算机网络之上的一套软件系统，它的基础是计算机网络，只是对用户来说，多个处理机的特性是透明的（用户看到的只是一个虚拟的单处理机，而实际上有多个处理机存在，单用户察觉不到多处理机的存在）。分布式系统将用户作业自动分配给各个处理机去处理；而在计算机网络系统中，用户需要某台计算机处理，必须指定这台计算机的地址，并且需要干预和管理这个网络系统。

由此把计算机网络定义为：凡将地理位置不同的、具有独立功能的多个计算机系统通过通信介质和设备连接起来，以功能完善的网络软件（网络协议、网络操作系统等）支持实现资源共享的系统，称为计算机网络系统。通信介质可以是有线的，如双绞线、同轴电缆、光纤等；也可以是无线的，如卫星通信、微波、红外线、激光等。

1.1.2 计算机网络的组成与拓扑结构

计算机网络是通过通信线路和设备互联的自治的计算机的集合。“互联”指两台相互连接的计算机能够相互交换信息。

一台控制机和多台从属机的系统不能称为网络，同样，一台大型计算机有多台远程终端和打印机，也不是网络。现在要解决的问题是计算机网络是如何组成的。

1. 计算机网络的组成

一般而言，计算机网络由计算机硬件、网络软件、通信设备和介质、网络上有关的信息与资源组成。计算机网络的三个主要组成部分为：若干个主机，它们分别为用户提供服务；一个通信子网，它主要由节点交换机和连接这些节点的通信链路所组成；一系列的协议。

（1）网络硬件

网络硬件是计算机网络的物质基础，计算机网络系统在物理上就是通过连接设备和通信线路将各种硬件连接起来。它由具有独立工作能力的计算机、网络设备、传输介质等硬件组成。

① 具有独立工作能力的计算机

计算机网络使用者使用的主要的网络资源是具有独立工作能力的计算机，它是计算机网络的核心。根据用途可以分为网络服务器和网络工作站。

网络服务器为使用者提供各种资源，一般情况下使用功能强大、运行速度快的计算机。服务器主要是为整个计算机网络服务的，而不针对某个用户，服务器的工作量比普通工作站的工作量要大很多。服务器与一般个人计算机的主要区别在于：运行速度快、存储容量大、稳定性和可靠性高。在服务器上运行的是计算机网络操作系统，比较常用的有Windows NT、UNIX、NetWare、Linux等。

网络工作站是供计算机网络用户使用网络的本地机，用户可以直接对其进行操作。一般网络上的工作站仅为使用者服务，用户通过操作工作站，借助网络访问网络服务器上的资源。

② 网络设备

计算机网络设备是构成计算机网络的一些部件，例如网卡、中继器、集线器、网桥、交换机、路由器、网关和调制解调器等。计算机通过网络设备连接起来，访问网络上的其他计算机。下面简单介绍各种网络设备的主要功能。

• 网卡

网卡又称网络适配器，是计算机与网络互联的接口设备。它的主要功能在于：产生网络信号、进行并行数据与串行数据的转换、控制数据缓存及存取、装配和拆卸数据包等。

• 集线器

因为信号在传输过程中会有损耗，为了在网络上远程传输数据，使用中继器（Repeater）将在传输介质上传输的信号放大。集线器（Hub）又称多口中继器，它的主要功能是用于扩展网络，将信号转发。使用集线器便于提高网络的稳定性和可靠性、改善网络的管理和维护。在集线器上，一个重要的参数是集线器的接口数，它指明了集线器能连接的计算机的数目，这里的计算机包括服务器、工作站、集线器等。如图 1-1 所示为集线器的连接。

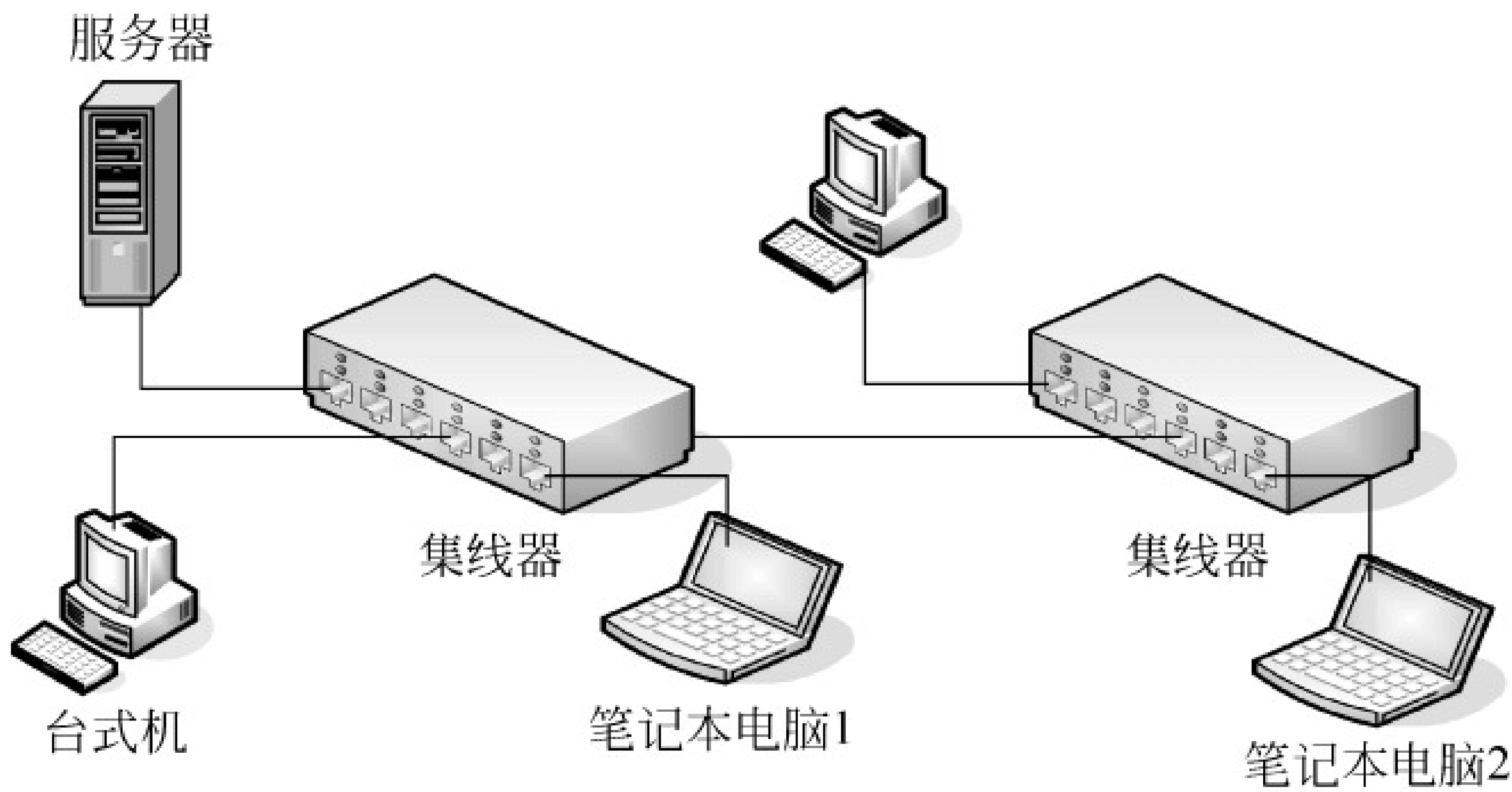


图 1-1　集线器的连接

无论是使用中继器还是集线器扩展网络距离，都要受 5—4—3 规则限制。该规则是指在一级联中，最多有 5 个网络段，其中通过 4 个中继器，只能有 3 个网络段上有计算机连接，另外 2 个网络段用来扩展网络距离。

• 网桥

集线器和中继器连接的网络仍然属于一个网络，而网桥用来连接两个同类型的局域网。所谓同类型是指网络的操作系统是相同的，与所用的传输介质和所采用的拓扑结构无关。网桥（Bridge）主要用于连接使用相同传输介质、通信协议和寻址方式的计算机网络。由于网桥具有信号过滤的作用，因而使用网桥可以将一个大型的计算机网络分成若干个子网，用来均衡各网段的负荷，以便提高网络的性能。网桥的连接如图 1-2 所示。

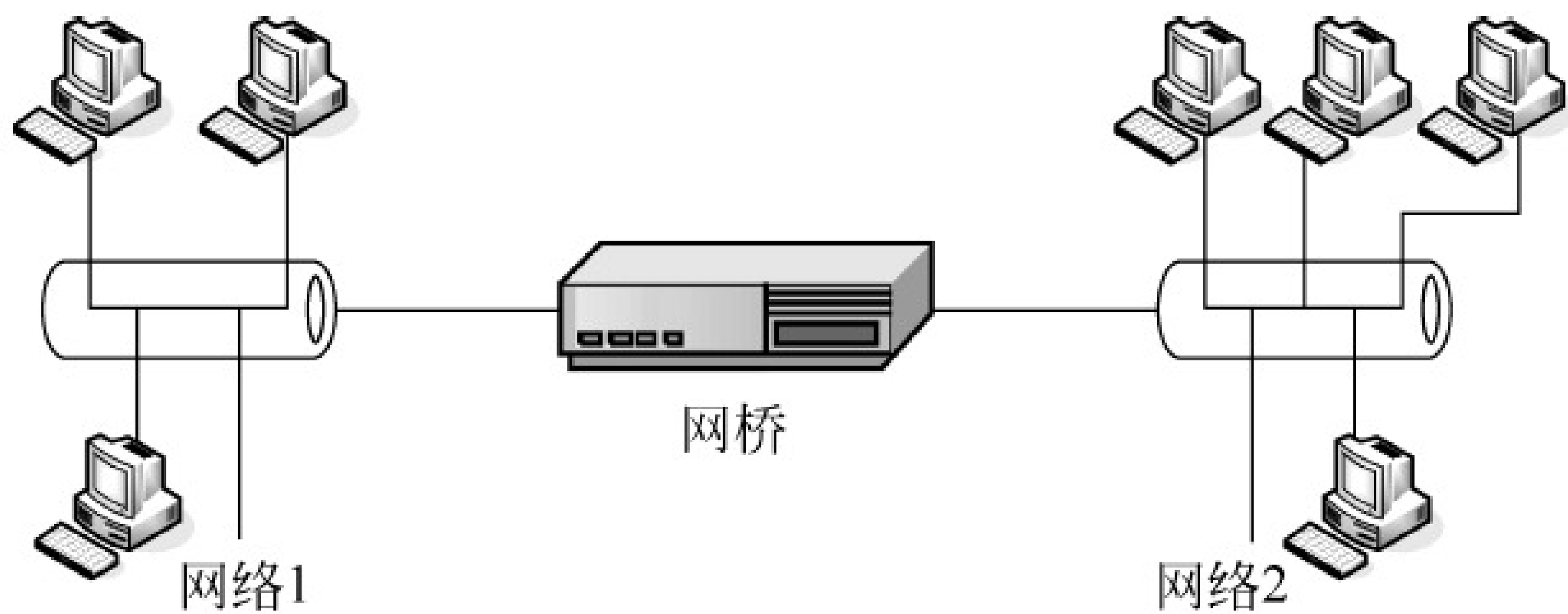


图 1-2　网桥的连接

• 交换机

交换机又叫交换式集线器，是一个多端口的网络，它能够接收由任一端口发来的数据帧，暂时存储，然后再转发到另一个端口。它的基本功能是路径选择和数据交换，通常由

软件完成路径选择，而由硬件连接来实现数据交换。交换机与网桥最大的区别在于：交换机能够在端口间同时建立多路连接，而网桥每次只能建立单路连接。交换机的连接如图 1-3 所示。

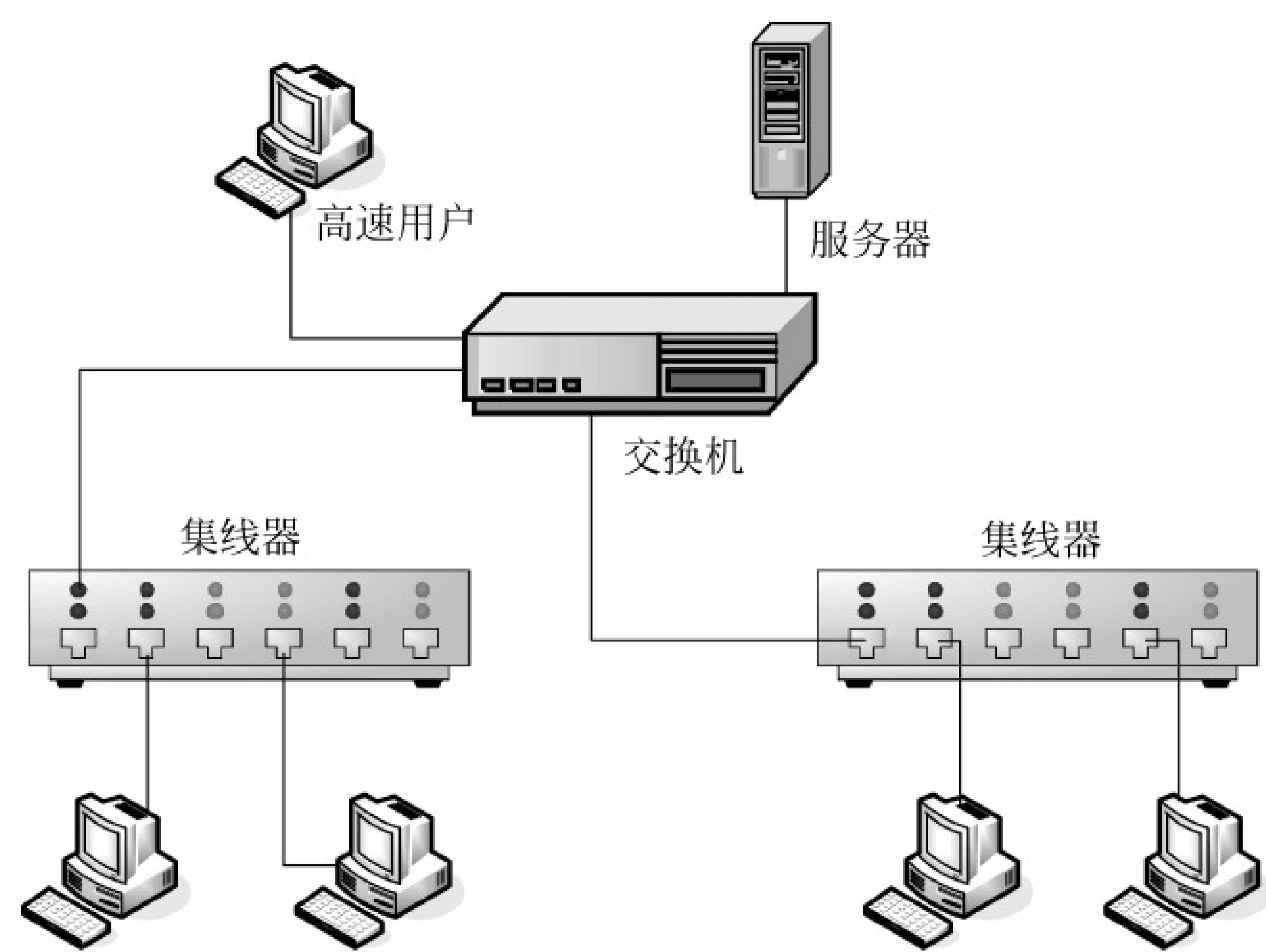


图 1-3 交换机的连接

另外，交换机还有一个突出的优点：它可以通过跳线或软件设定，来实现一个端口数据向多个端口转发。该特点的好处就是能够组建虚拟局域网，它可以根据网络用户的工作性质（而不考虑其实际地理位置），通过软件将可能位于多个物理网络中的用户设置于同一广播域（虚拟局域网）内。这可以简化网络的管理，并可能实施灵活的网络配置。

• 路由器

路由器（Router）是连接多个同类网络或连接局域网和广域网的网络设备。路由器除了具备网桥的功能外，还具备路由选择功能。在计算机网络系统运行中，路由器的主要工作就是为经过本路由器的计算机传输报文寻找一条最佳或较好的传输路径，并将报文传送到目的站点。路由器的连接如图 1-4 所示。

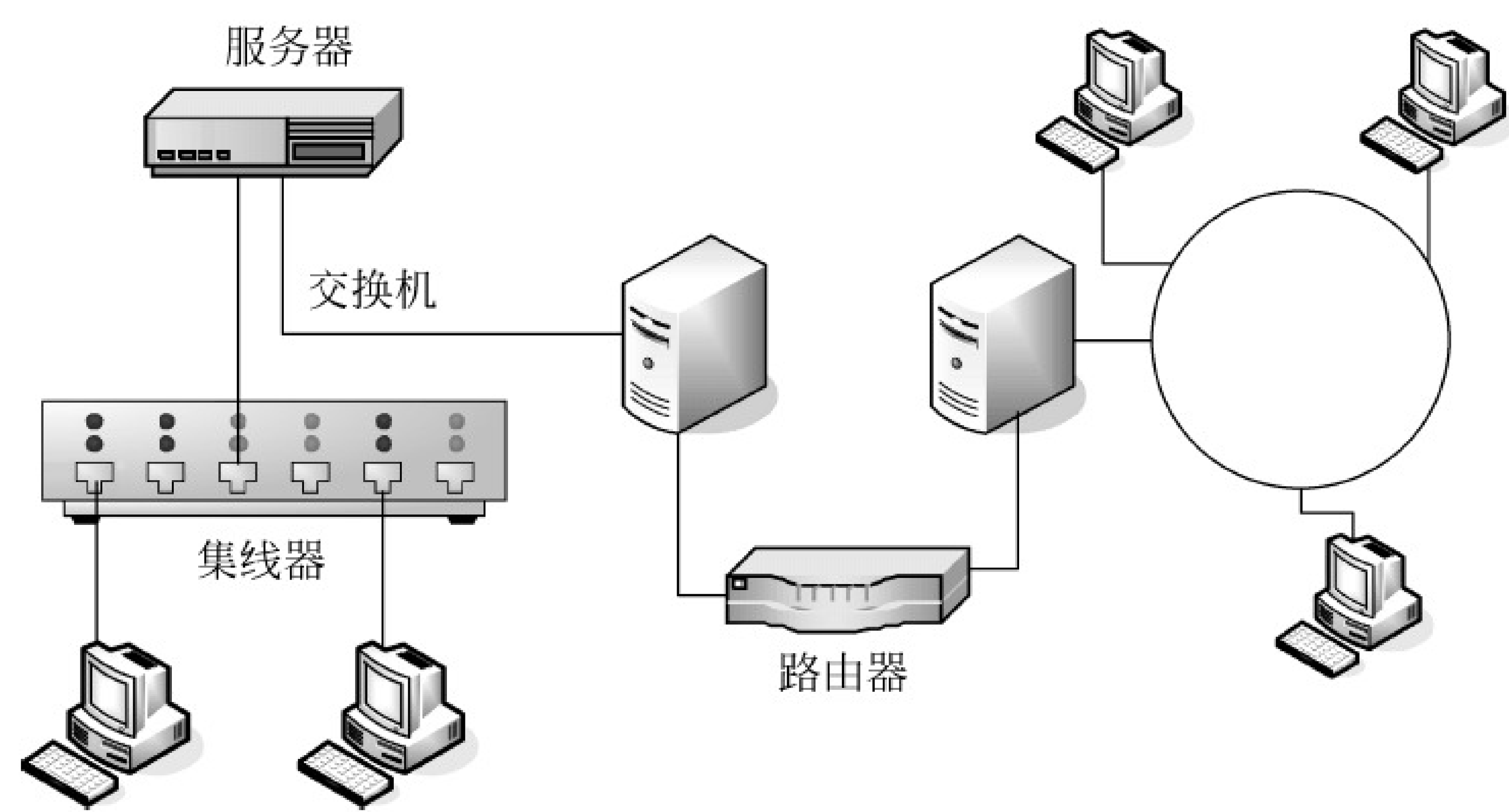


图 1-4 路由器的连接

• 网关

网关(Gateway)在计算机网络中主要用来连接不同类型的网络,为这些不同的网络间提供相互的协议变换,并将数据按照新的协议重新分组之后再向下传送。网关是一种协议转换器,有时也称为协议路由器。常见的网关路由协议有外部网关协议 EGP,边界网关协议 BGP,内部网关路由协议等。

• 调制解调器

调制解调器(Modem)一般用于家庭计算机通过电话线联网,它的主要作用在于通信过程中实现模拟信号和数字信号的相互转换。调制解调器分为内置调制解调器和外置调制解调器两种。

③ 网络传输介质

传输介质是网络通信所使用的信号线路,分为有线介质和无线介质两类。有线介质包括同轴电缆、双绞线和光纤等,现在最常用的是双绞线和光纤;无线介质有微波、红外线和激光等。各种传输介质的特点和连接方式在后面再详细介绍。

(2) 网络软件

网络软件主要用于合理地调度、分配、控制网络系统资源,并采取一系列的保密安全措施,保证系统运行的稳定性和可靠性。它包括网络通信协议软件、网络操作系统和网络应用软件等。

① 网络通信协议与协议软件

网络通信协议用于支持计算机与相应的网络互联,并与该网络上的其他计算机按该协议进行通信。简单地说,协议是通信双方为了进行通信所做的约定和对话规则。它包括三个方面的内容:语义、语法和时序。

- 语义:各种控制信息的含义、需要完成的动作和做出的响应,即协议元素的类型。
- 语法:用户数据与控制信息的结构和格式,即协议元素的格式。
- 时序:对事件实现顺序的详细说明。时序包括执行顺序和速度匹配两个方面的内容。

网络协议对计算机网络是不可缺少的,一个功能完备的计算机网络必须具备一套复杂的协议集。典型的网络通信协议有局域网的 IEEE 802.2 系列协议,TCP/IP 协议,IPX/SPX 协议等,它们均有各自对应的协议软件。现阶段网络协议软件大都被包含于操作系统中。

通信软件的主要目的是使用户不需要了解很多通信规程,方便用户控制的应用程序,同时与多个站点进行通信,并管理和加工大量通信数据的输入和输出。

② 网络操作系统

网络操作系统(Network Operating System,NOS)是管理网络资源的系统软件,是网络用户与计算机网络之间的接口。网络操作系统是计算机网络系统的核心部分,通过它对各种网络资源、网络用户等进行管理。网络操作系统的主要部分存放在服务器上,它的主要功能是服务器管理、通信管理,以及一般多用户、多任务操作系统所具有的功能。网络操作系统中既有单机操作系统的处理机管理、内存管理、文件管理、设备管理和作业管理等功能,也有对整个网络的资源进行协调管理,实现计算机之间高效可靠地通信,提供

各种网络服务和为网络用户提供便利的操作与管理平台等网络管理功能。一个典型的网络操作系统应有如下特征。

- 与硬件独立：网络操作系统可以在不同的网络硬件上运行。
- 网桥/路由连接：内置有网桥/路由功能，从而能和其他网络连接。
- 支持多用户：支持多个用户同时使用网络资源，并能给应用程序及其数据文件提供足够的、标准化的保护。
- 网络管理：支持网络实用程序及其管理功能，如系统备份、安全管理、容错、性能监控等。
- 安全和存取控制：对用户资源进行控制，并提供控制用户对网络的访问方法。
- 具备操作系统的基本功能：如任务管理、缓冲区管理、文件管理、磁盘和打印机等外部设备的管理。

③ 网络应用软件

网络应用软件是构建在网络操作系统之上的应用程序，它扩展了网络操作系统的功能，不同的网络应用软件，可满足用户在不同情况下的需求。如网络数据库系统、网络邮件系统等。

2. 计算机网络的逻辑组成

按照计算机网络的逻辑功能，可以认为计算机网络由资源子网与通信子网两部分组成，如图 1-5 所示。

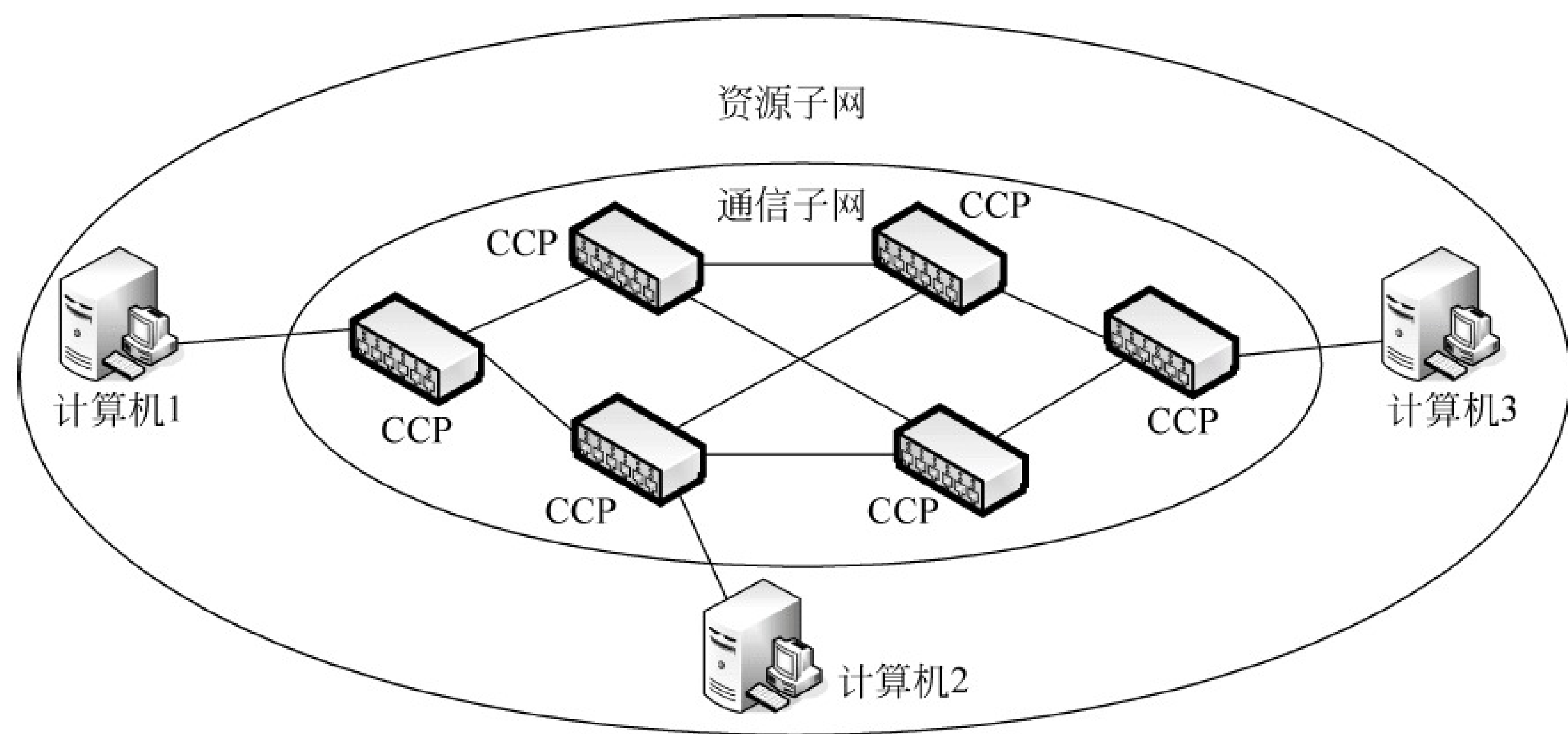


图 1-5　资源子网与通信子网

资源子网又叫数据处理子网，包括网络中独立工作的计算机、外围设备、各种软件资源。负责处理整个网络数据，并向网络用户提供各种网络资源和网络服务等。

通信子网又叫数据通信子网，也称数据通信提供者。它是网络中的数据通信系统，它由用于信息交换的网络节点处理机和通信链路组成。主要负责通信处理工作，如网络中的数据传输、加工、转发和变换等。不同的网络会有不同的通信子网，其任务是在端节点之间传送报文。在局域网中，把传输介质和网卡以及集线器等作为通信子网。广域网中，通信子网还应该包括通信处理机。

如果用户只是访问本地计算机，则只在资源子网内部进行，无须通过通信子网。如果用户要访问异地计算机资源，则必须通过通信子网。

3. 网络拓扑结构

网络中各节点相互连接的方法和形式称为网络拓扑。它指明了网络中计算机系统的几何排列形状，反映了网络各部分的结构关系和整体结构，影响着整个网络的设计、可靠性、功能和通信费用等重要指标，并与传输介质、介质访问控制方法等密切相关。

计算机网络的拓扑结构有星型、环型、总线型、树型以及网状结构等基本形式。

（1）星型结构

星型结构由中央节点和通过点到点通信链路连接到中央节点的各个站点组成，如图 1-6 所示。中央节点控制全网的通信，任何两个节点之间的通信都要通过中央节点。星型结构的中央节点一般是交换机或集线器（Hub）。中央节点执行集中式通信控制策略，因此，中央节点相当复杂，而各个站点的通信处理负担都很小。星型结构采用的交换方式有电路交换和报文交换两种。

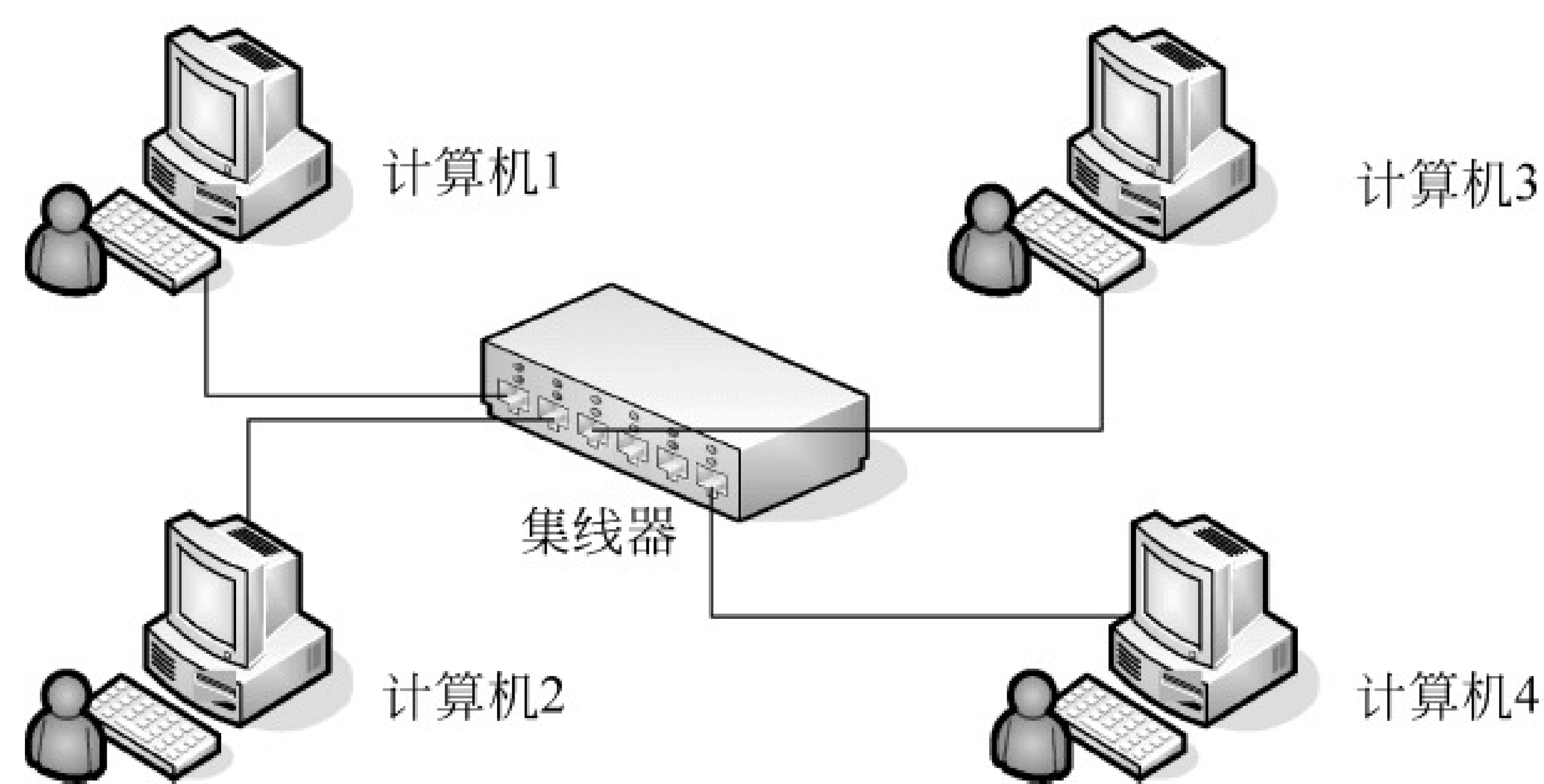


图 1-6　星型结构

星型结构具有以下优点：

- 控制简单。任何一个站点只和中央节点相连接，因而介质访问控制方法很简单，访问协议也十分简单。
- 故障诊断和隔离容易。中央节点对连续线路可以逐一地隔离来进行故障检测和定位，单个连接点故障只影响一个设备。
- 方便服务。中央节点可以方便地对各个站点提供服务，或者重新配置网络。

星型结构的缺点：电缆长度较长，安装工作量大；中央节点负担重，容易成为系统“瓶颈”；各个站点的分布处理能力较低。

现阶段以高速交换设备为中心的星型拓扑结构在局域网组建中使用越来越广泛。

（2）环型结构

环型结构由站点和连接站点的通信链路组成一个闭合环。任何两个节点之间都要通过环路相互通信，点到点通信线路形成闭合环路。环中的数据逐站传送，绕环一周才能实现相互通信。环型结构中各主计算机地位相等，网络中的信息流向只能是单方向的。环型结构如图 1-7 所示。在环型结构中，数据以分组形式发送。

环型结构的优点：电缆长度比星型结构要短，可以使用光纤，传输延时确定。

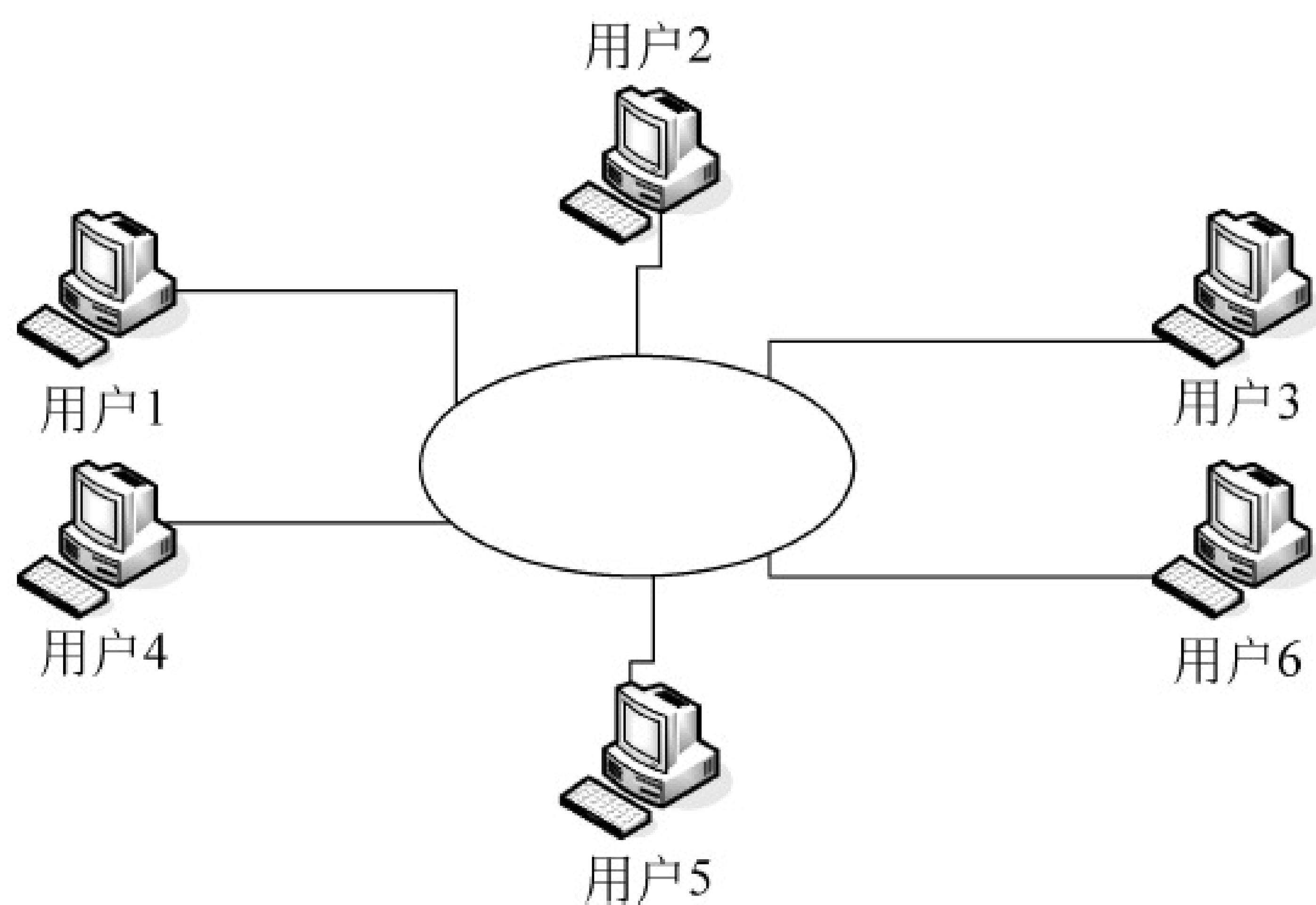


图 1-7　环型结构

环型结构的缺点：环中每个节点的故障会引起全网的故障，故障检测困难，节点的加入和撤出过程复杂。

（3）总线型结构

总线型结构采用一个共享信道作为传输介质，所有站点都通过相应的硬件接口直接连到总线上。任何一个站点发送的数据信号都沿着传输介质传播，而且能被所有站点接收。总线型结构如图 1-8 所示。

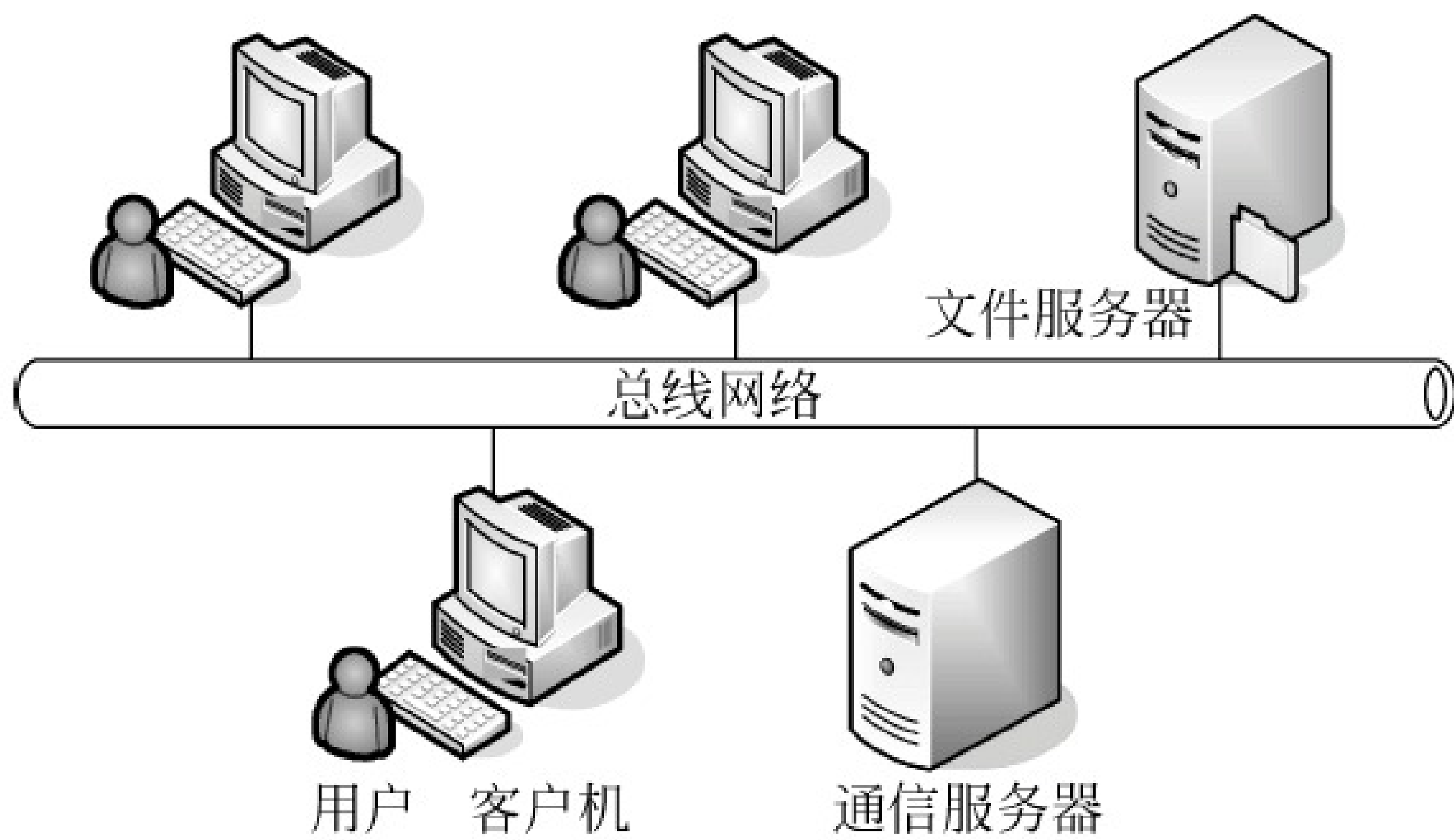


图 1-8　总线型结构

总线型结构的优点：所需要的电缆数量少，总线结构简单，易于扩充。

总线型结构的缺点：总线的传输距离有限，通信范围受到限制；故障诊断和隔离比较困难；信息延迟不确定，不能适用于实时通信。

（4）树型结构

可以认为树型结构是一种多总线型结构，如图 1-9 所示。根节点接收各站点发送的数据，然后再广播发送到全网。

树型结构的优点：易于扩展，故障隔离容易。

树型结构的缺点：各个节点对根节点的依赖性太大，若根节点发生故障，则全网无法正常工作。

（5）网状拓扑结构

网状拓扑结构网络中的节点之间的连接是任意的、无规律的，如图 1-10 所示。

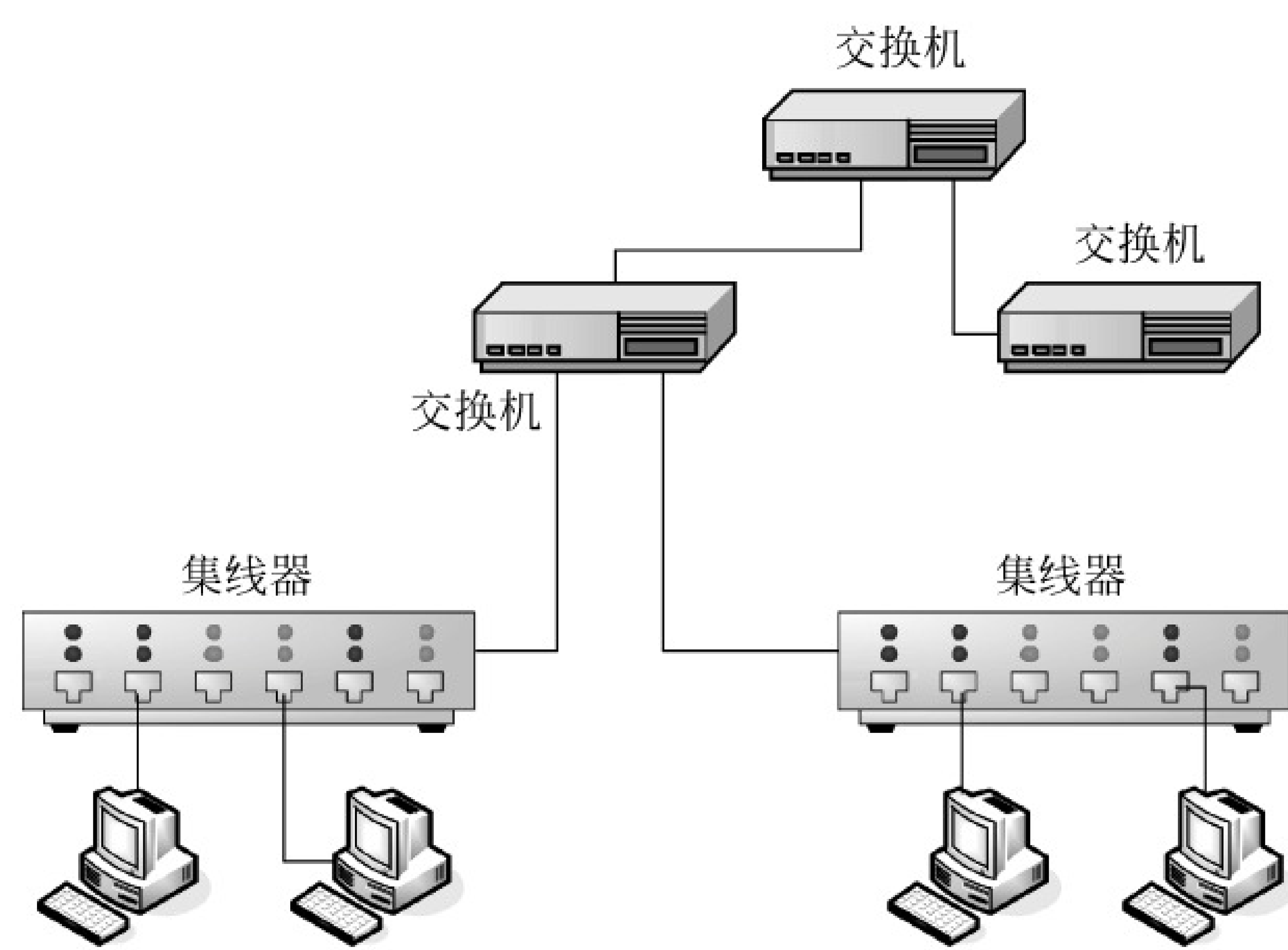


图 1-9　树型结构

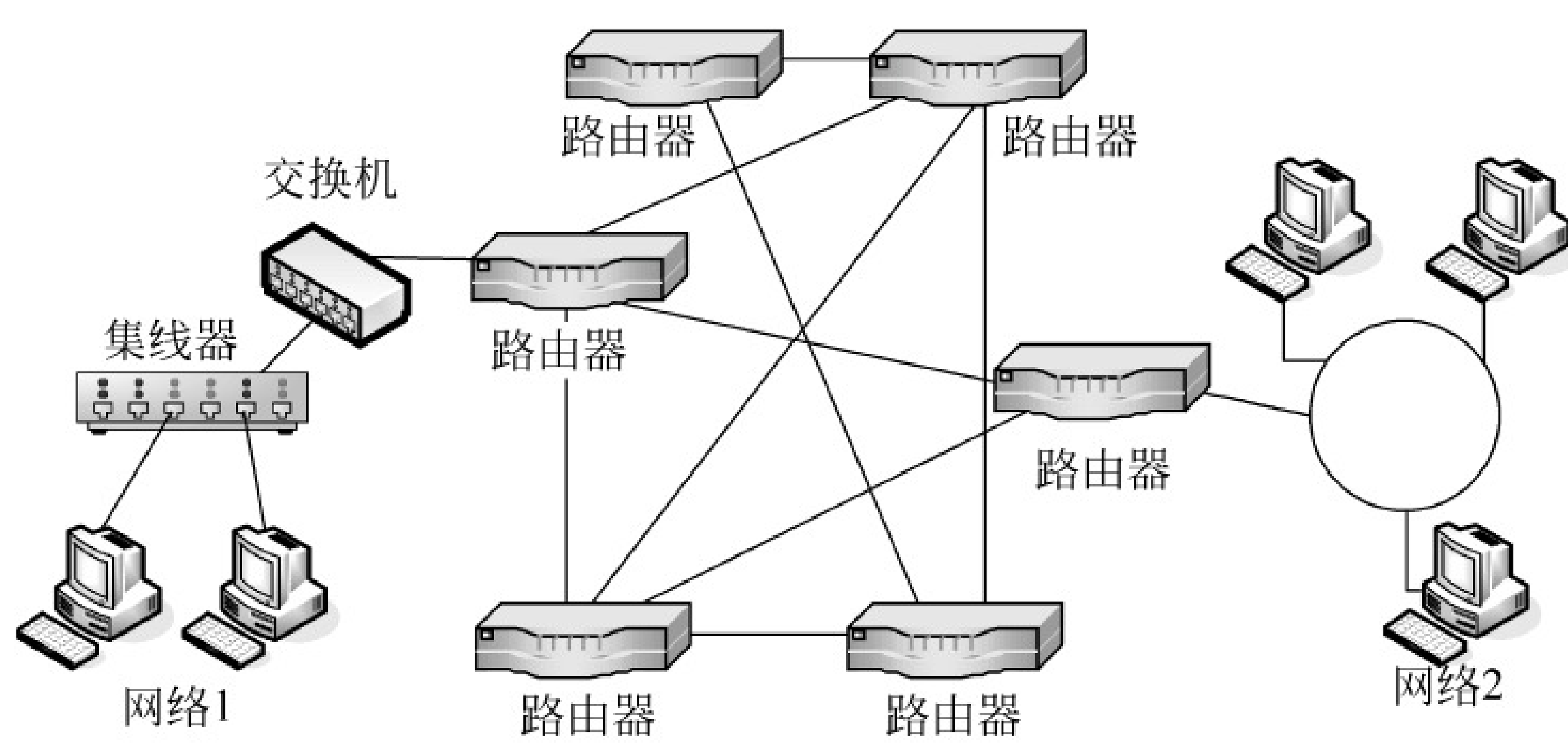


图 1-10　网状拓扑结构

在网状拓扑结构中,节点之间可能有多条路径选择,因此,其中个别节点发生故障对整个网络影响不大。网状结构的主要优点是系统可靠性高,它的缺点是网络系统结构复杂,一般成本较高。

以上这些网络的拓扑结构根据通信方式可以归结为两类:点到点线路通信子网的拓扑和广播信道通信子网的拓扑。点到点线路通信子网又称为存储转发式通信子网,它的特点是任何两个非直接相连的节点必须通过其他节点进行转发,某个节点接收到信息并存储,等线路空闲再转发出去。广播信道通信子网又称为共享信道通信子网,它的特点是任意两个节点都直接相连,信息采用位流的形式,一个节点发送信息,其他节点处于接收状态。

局域网的基本拓扑结构有总线型、环型和星型三种,广域网则大多数采用网状拓扑结构,而 Internet 则采用树型结构。

1.1.3　计算机网络的功能

1. 数据通信

数据通信即数据传送,是计算机网络的最基本功能之一。从通信角度看,计算机网络

其实是一种计算机通信系统。作为计算机通信系统,能实现下列重要功能。

(1) 传输文件

网络能快速地在计算机与计算机之间进行文件复制和传送。

(2) 使用电子邮件(E-mail)

用户可以将计算机网络作为邮局,向网络上的其他计算机用户发送备忘录、报告和报表等。虽然在办公室使用电话是非常方便的,但 E-mail 可以向不在办公室的人传送消息,而且还提供了一种无纸办公的环境。

2. 资源共享

资源共享包括硬件、软件和数据资源的共享,它是计算机网络最有吸引力的功能。资源共享是指网上用户能够部分或全部地使用计算机网络资源,使计算机网络中的资源互通有无、分工协作,从而大大地提高各种硬件、软件和数据资源的利用率。

3. 提高计算机系统的可靠性和可用性

计算机系统可靠性的提高主要表现在,计算机网络中每台计算机都可以依赖计算机网络相互作为后备机,一旦某台计算机出现故障,其他的计算机可以马上承担起原先由该故障机所担负的任务,避免了系统的瘫痪,使得计算机的可靠性得到了大大的提高。

计算机可用性的提高是指当计算机网络中某一台计算机负载过重时,计算机网络能够进行智能的判断,并将新的任务转交给计算机网络中较空闲的计算机去完成,这样就能均衡每一台计算机的负载,提高了每一台计算机的可用性。

4. 易于进行分布处理

在计算机网络中,每个用户可根据情况合理选择计算机网内的资源,以就近的原则快速地处理。对于较大型的综合问题,通过一定的算法将任务分交给不同的计算机,从而达到均衡网络资源,实现分布处理的目的。此外,利用网络技术,能将多台计算机连成具有高性能的计算机系统,以并行的方式共同来处理一个复杂的问题,这就是当今称为协同式计算机的一种网络计算模式。

任务完成:通过学习前面的知识,完成任务 1.1 就是水到渠成的事情了。任务 1.1 要求将实验室中的 20 台个人计算机,1 台文件服务器,1 台共享打印机,组成计算机网络的形式,实现资源共享。用最简单的星型结构方式,用一个 24 口的集线器将所提供的设备连接起来,构建一个星型网络,如图 1-11 所示。

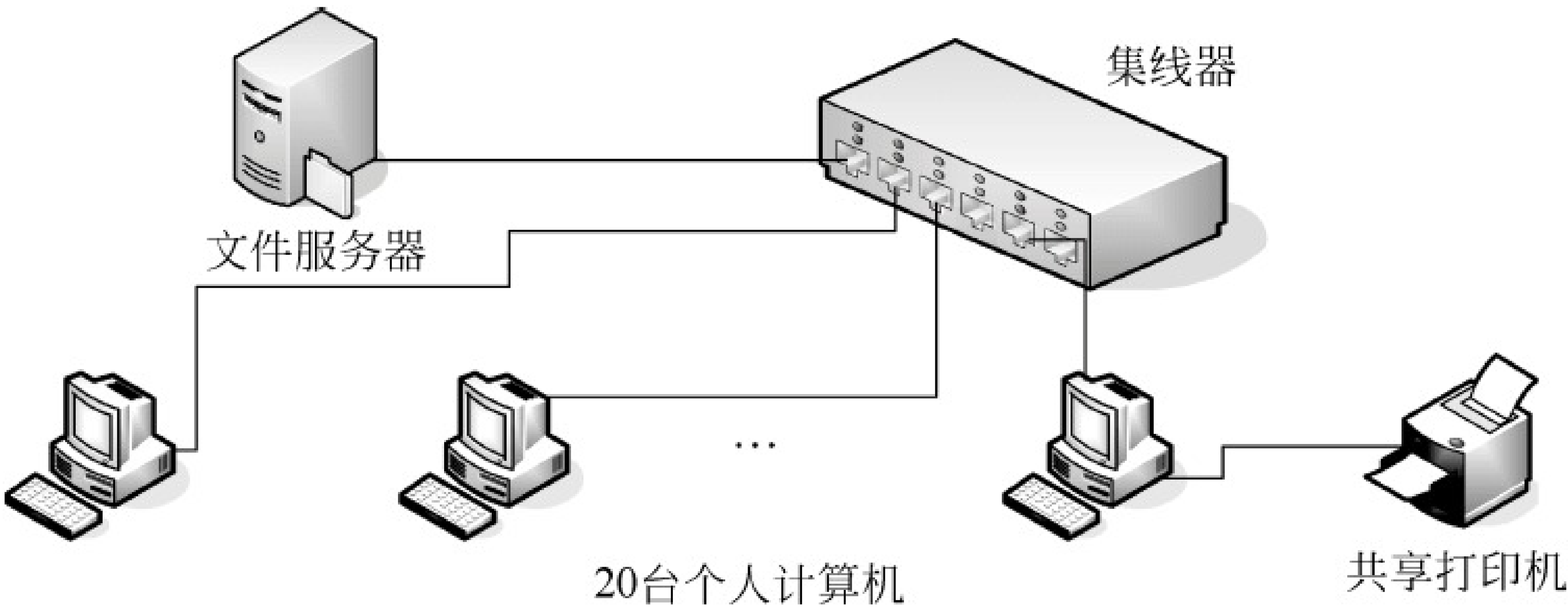


图 1-11　星型网络拓扑

任务 1.2　选择网络类型

任务描述：某部门有 5 台 PC，其中 1 台性能较高，在不关心安全性的情况下，采用什么样的网络使得各台计算机能够互相通信，并能够使用性能较高的计算机的资源？每台计算机各自的角色是什么？

根据网络中各台计算机的作用不同，计算机网络分为不同的形式。某网络中各台计算机的作用是相同的，具有平等的地位，那么该网络称为对等网。如果在网络中某台计算机性能较高，为其他计算机提供服务，那么这种网络称为客户机/服务器网络。这两种网络哪一种更符合任务 1.2 的需求呢？下面先来详细了解这两种网络。

1.2.1　对等网络

所谓对等网络（简称对等网），即网络中各台计算机都有相同的功能，无主从之分，网络中任意一台计算机既可以作为网络服务器，为其他计算机提供资源；也可以作为工作站，以分享其他服务器的资源。任意一台计算机均可同时兼作服务器和工作站，也可只作其中之一。

“对等网”也称“工作组网”，因为它不像企业专业网络中那样是通过域来控制的，在对等网络中没有“域”，只有“工作组”，因此，在具体网络配置中，只需配置工作组。很显然，“工作组”的概念远没有“域”那么广，所以对等网所能承载的用户数也是非常有限的。

在对等网中，计算机的数量通常不会超过 20 台，所以对等网相对比较简单。在对等网络中，除了共享文件之外，还可以共享打印机，对等网上的打印机可被网络上的任一节点使用，如同使用本地打印机一样方便。因为对等网不需要专门的服务器来做网络支持，也不需要其他组件来提高网络的性能，因而对等网的价格相对要便宜很多。

对等网的主要特点如下。

(1) 网络用户较少，一般在 20 台计算机以内，适合人员少、网络应用较多的中小企业。

(2) 网络用户都处于同一区域中。

(3) 对于网络来说，网络安全不是最重要的问题。它的主要优点是：网络成本低、网络配置和维护简单；主要缺点是：网络性能较低、数据保密性差、文件治理分散、计算机资源占用大。

虽然对等网结构比较简单，但根据具体的应用环境和需求，对等网也因其规模和传输介质类型的不同，其实现的方式也有多种，下面分别进行介绍。

1. 两台机的对等网

这种对等网的组建方式比较多，在传输介质方面既可以采用双绞线，也可以使用同轴电缆，还可采用串行、并行电缆，所需网络设备只需相应的网线（或电缆）和网卡。假如采用串行、并行电缆还可省去网卡的投资，直接用串行、并行电缆连接两台计算机即可，显然这是一种最廉价的对等网组建方式。但这种采用串行、并行电缆连接的网络的传输速率

非常低，并且串行、并行电缆制作比较麻烦，在网卡如此便宜的今天，这种对等网连接方式比较少用。

2. 三台机的对等网

假如网络所连接的计算机不是两台，而是三台，则此时就不能采用串行、并行电缆连接了，而必须采用双绞线或同轴电缆作为传输介质，而且网卡是不能少的。假如是采用双绞线作为传输介质，根据网络结构的不同又可有两种方式：一种是采用双网卡网桥方式，就是在其中一台计算机上安装两块网卡，另外两台计算机各安装一块网卡，然后用双绞线连接起来，再进行有关的系统配置即可。另一种是添加一个集线器作为中继设备，组建一个星型对等网，三台计算机都用双绞线连接直接与集线器相连。从这种方式的特点来看，虽然可以省下一块网卡，但需要购买一个集线器，网络成本会较前一种高些，但性能要好许多。

假如采用同轴电缆作为传输介质，则不需要购买集线器了，只需把三台计算机用同轴电缆网线直接串联即可。虽然也只需三块网卡，但因同轴电缆较双绞线贵些，所以总的投资与用双绞线差不多。

3. 多于三台机的对等网

对于多于三台计算机的对等网组建方式只能有两种：①采用集线设备(集线器或交换机)组成星型网络；②用同轴电缆直接串联。虽然这类对等网也可采用双网卡网桥方式，就是在除了首、尾两台计算机外都采用双网卡配置，但这种方式因要购差不多两倍的网卡，成本较高；且双网卡配置对计算机硬件资源要求较高，所以很少有人会用这种方式来实现多台计算机的对等网互联。

以上介绍的是对等网的硬件配置，在软件系统方面，对等网更是非常灵活，几乎所有操作系统都可以配置对等网，包括网络专用的操作系统，如 Windows NT Server/2000 Server/Server 2003，Windows 9X/ME/2000Pro/XP 等也都可以，甚至早期的 DOS 系统也可以。

1.2.2 客户机/服务器网络

客户机/服务器网络是一种基于服务器的网络，与对等网相比，基于服务器的网络提供了更好的运行性能，并且可靠性也有所提高。在基于服务器的网络中，不必将工作站计算机的硬盘与他人共享。实际上，如果想与某个人共享一份文件，就必须先将文件复制到服务器的硬盘上(或者一开始就在服务器上生成该文件)，这样别人才能访问这份文件。共享数据全部都集中存放在服务器上。客户机/服务器的一个典型应用就是数据库的应用。

任务完成：根据任务 1.2 的要求，我们可以构建一个客户机/服务器网络，如图 1-12 所示。其中，一台性能较高的计算机作为服务器，为其他客户机提供服务。可以考虑用集线器及双绞线将各种设备连接起来，在服务器上安装网络操作系统及相应的服务器组件，并进行相应的配置。同时客户机进行正确的网络设置，即可实现通信。

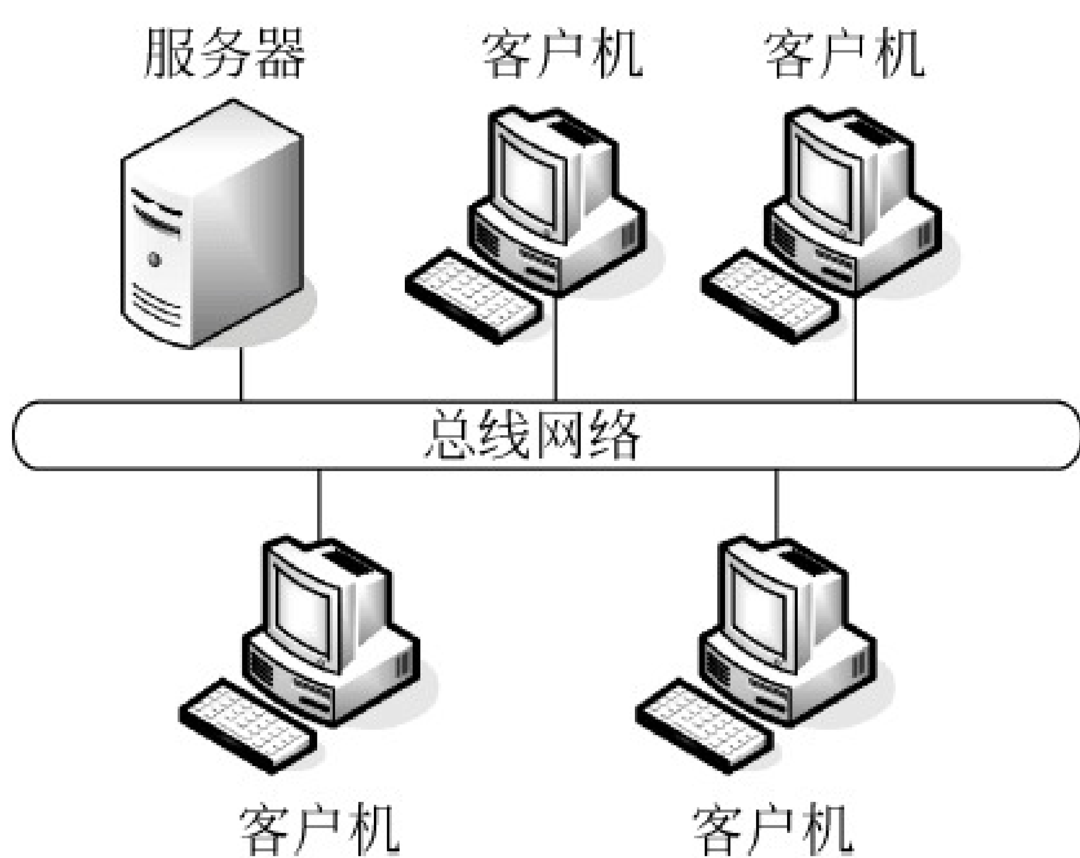


图 1-12　客户机/服务器网络

知识拓展——计算机网络的历史与发展

1946 年世界上第一台电子计算机的诞生，在当时是很大的创举，但是任何人都没有预测到，60 年后的今天，计算机在社会各个领域的应用和影响是如此广泛与深远。当 1969 年 12 月世界上第一个数据包交换计算机网络 ARPANET 出现时，也不会有人预测到，计算机网络在现代信息社会中扮演了如此重要的角色。ARPANET 已从最初的 4 个节点发展为横跨全世界一百多个国家和地区、连接有几万个网络、几百万台计算机、几亿个用户的互联网(Internet)。互联网是当前世界上最大的国际性计算机互联网络，而且还在发展之中。

纵观计算机网络的发展历史可以发现，它和其他事物的发展一样，也经历了从简单到复杂，从低级到高级的过程。在这一过程中，计算机技术与通信技术紧密结合，相互促进，共同发展，最终产生了计算机网络。

1. 具有通信功能的单机系统

这是计算机网络发展的雏形，主机系统完成数据处理和通信，如图 1-13 所示。

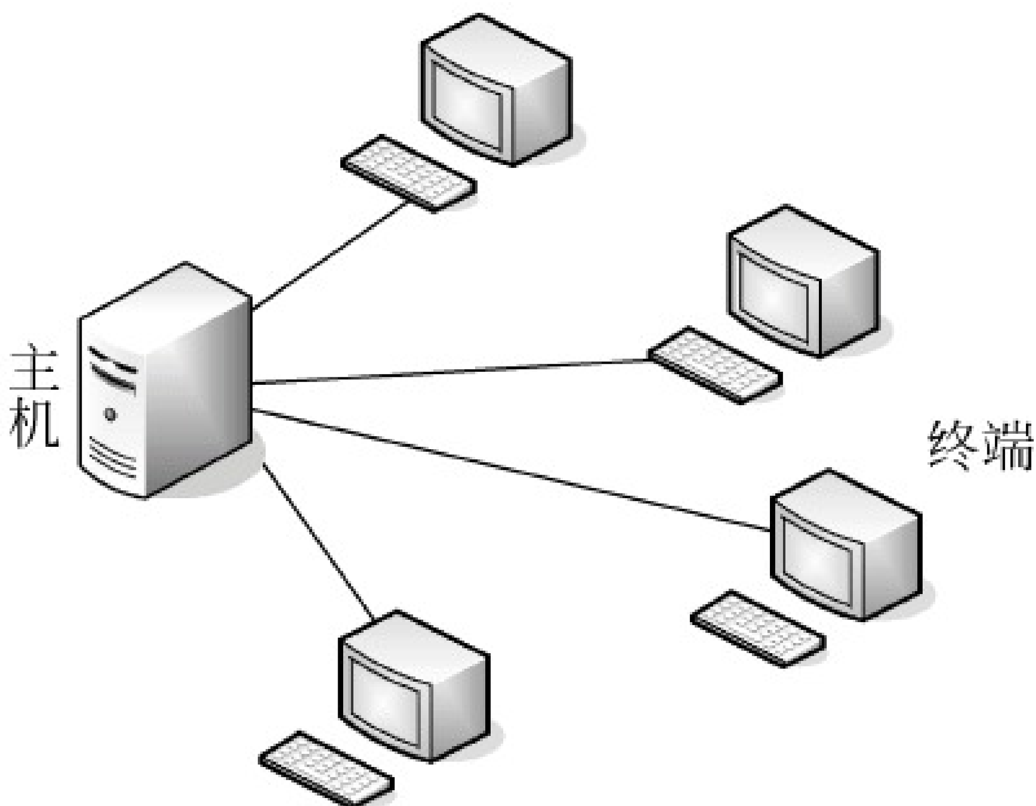


图 1-13　具有通信功能的单机系统

2. 具有通信功能的多机系统

具有通信功能的单机系统，计算机主机既要处理数据又要承担通信任务，并且当终端数目较多时，要连接多条线路，造成了线路的利用率较低。具有通信功能的多机系统在主机前增加了一台前置处理机(CCP)，专门用于通信，主机主要用于数据的处理；另外，在终端集中的区域增加了集线器，提高了线路的利用率，如图 1-14 所示。

3. 计算机—计算机网络

如图 1-15 所示为计算机—计算机网络(当前的各种网络都是计算机—计算机网络)。

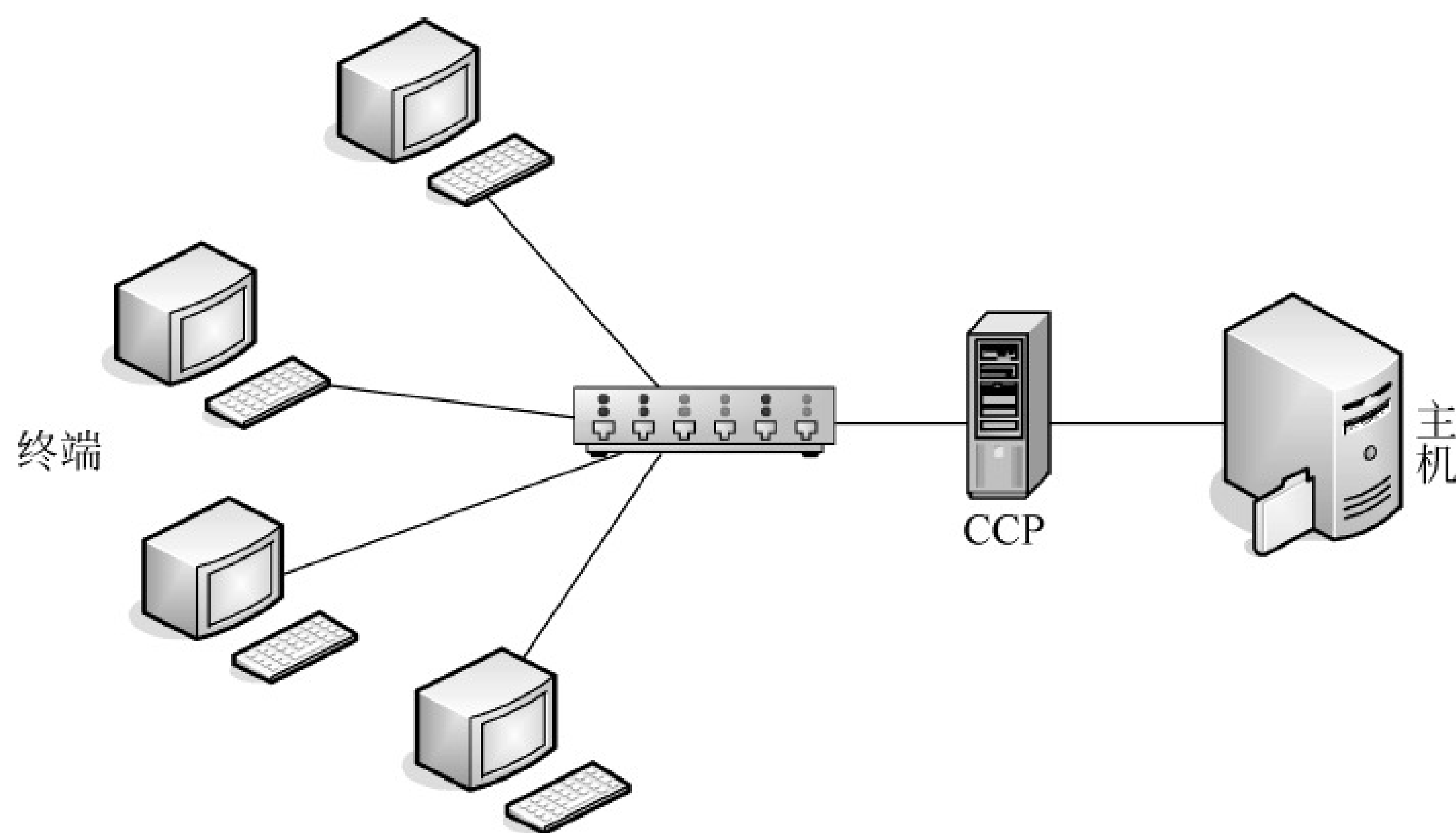


图 1-14　具有通信功能的多机系统

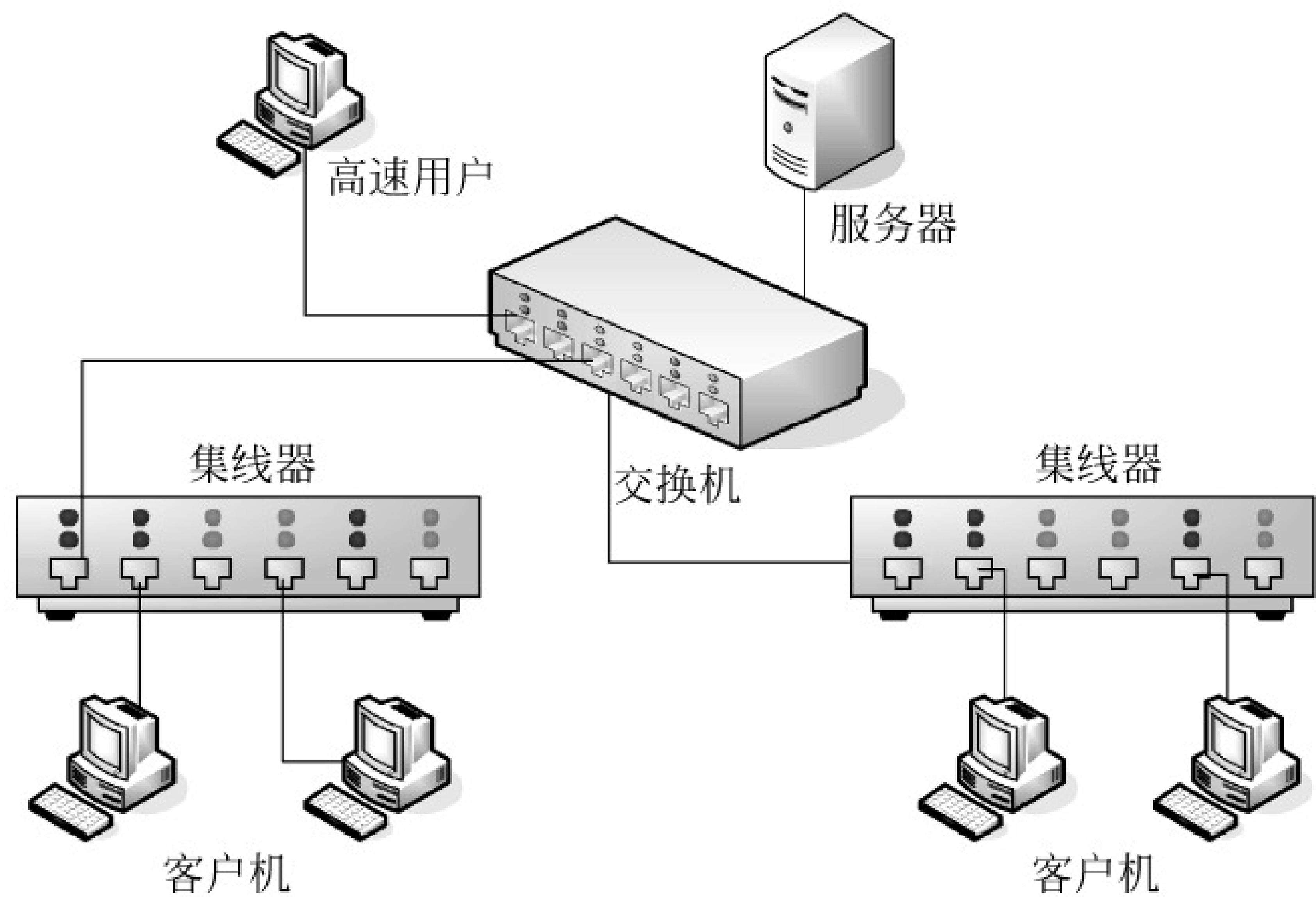


图 1-15　计算机—计算机网络

实训 1　绘制实验室网络拓扑图

1．实训目的

通过绘制网络拓扑图,加深对网络结构的理解。

2．实训内容

观察本校计算机网络实验室的网络连接,根据实际情况画出实验室的网络拓扑结构图。

3．实训步骤

(1) 识别计算机网络实验室的设备及其功能。

(2) 分析计算机网络实验室中计算机与网络设备的连接情况。

(3) 用拓扑图形式画出计算机网络实验室的网络结构。

4．实训要求

(1) 在拓扑图中标注实验设备及其作用。

(2) 分析计算机网络实验室的拓扑结构,分析其优缺点。

习　题　1

1. 选择题

(1) 计算机网络最突出的优点是(　　)。

A. 精度高　　B. 内存容量大　　C. 运算速度快　　D. 共享资源

(2) 在组建局域网时,经常采用的拓扑结构是(　　)。

A. 星型　　B. 总线型　　C. 环型　　D. 网状

(3) 在同一个信道上的同一时刻,能够进行双向数据传送的通信方式是(　　)。

A. 单工　　B. 半双工　　C. 全双工　　D. 上述三种均不是

(4) 以下(　　)不属于计算机网络的应用。

A. 电子邮件　　B. 网上交易　　C. 文字处理　　D. IP 电话

(5) 下列(　　)句子最佳地描述了星型网络。

A. 比其他拓扑结构需要的电缆更少

B. 单条电缆的损坏会使整个网络瘫痪

C. 重新配置比其他拓扑结构困难

D. 集中方式的监视和管理

2. 填空题

(1) 计算机网络系统由通信子网和________子网组成。

(2) 将模拟信号和数字信号进行相互转换的设备是________。

(3) 在采用电信号表达数据的系统中,数据有数字数据和________两种。

3. 简答题

(1) 什么是计算机网络? 它由哪些部分组成? 它的主要应用是什么?

(2) 简述星型拓扑结构的优缺点。

模块 2　网络数据通信基础

任务 21　制作网线

任务描述：计算机网络技术是计算机技术与通信技术相结合的产物，计算机之间要通过传输介质才能够实现数据通信。那么计算机之间是如何连接的？使用什么样的传输介质呢？通过下面的学习来实现常用网线的制作。

2.1.1　数据通信的基本概念

数据通信是实现计算机之间信息传递的基础。下面简单介绍与数据通信相关的基本概念。

(1) 信息是客观事物属性和相互联系特性的表征，它反映了客观事物的存在形式和运动状态，是对客观事物存在形式的一种反映。例如我们常说的文字信息、语音信息、图像信息和数据信息等。

(2) 数据是数字化的信息。分为模拟数据和数字数据：模拟数据取值是连续的，如语音强度、电压高低、温度等；数字数据取值是离散的，如文本信息和整数值。

(3) 信号是数据的电、磁、光等形式的编码形式。信号可分为数字信号和模拟信号。模拟信号是指在时间上和幅度取值上都连续变化的信号。数字信号是指在时间上离散的、在幅值上经过量化的信号。如计算机输出的脉冲信号是数字信号，电话机输出的信号就是频率和振幅连续改变的模拟信号。

(4) 信源是指在通信的过程中产生和发送信号的设备或计算机。

(5) 信宿是指在通信的过程中接收和处理信息的设备或计算机。

(6) 信道是指信源和信宿之间的传输线路和传输设备，分为物理信道和逻辑信道。在同一物理信道上可以提供多条逻辑信道，而在每一逻辑信道上只允许一路信号通过。

(7) 信号变换器的作用是将信源发出的信息变换成适合在信道上传输的信号，如编码器、调制器、译码器或解调器等。

(8) 码元是承载信息的基本信号单位。模拟信号的一个波形单元称为一个码元。若用脉冲信号表示数据的有效值状态，一个单位脉冲就是一个码元。

(9) 信号传输速率 B(波特率)：指在有效带宽上单位时间传送的码元数，单位是波特(baud)。

(10) 数据传输速率 S(比特率)：指单位时间内所传送的二进制代码的有效位数，单位是 bps，另外常用的还有 kbps、Mbps 等。

信号传输速率与数据传输速率之间的关系为：

$$S=B\log_2 N$$

其中，N 为一个码元所取的有效离散值的个数。在二进制中，脉冲只有 0 或 1 两种状态，即 $N=2$，也就是说一个码元只携带一位二进制数据(0 或 1)，所以这时信号速率 S 与调制速率 B 是一致的。打个比方，假如信号传输速率是邮局单位时间内寄送的普通信封数，那么数据传输速率就是单位时间内邮局寄出的信封中信纸的张数。

(11) 带宽是指物理信道的频带宽度，即信道允许的最高频率和最低频率之差，单位为赫[兹](Hz)。有效带宽是指单位大小的信号通过信道时，幅度衰减至原信号的 0.707 倍时，最高频率和最低频率之差。通常所说的带宽是指有效带宽。

(12) 信道容量是用来表征一个信道传输数字信号的能力，它以数据传输速率作为指标，即信道所能支持的最大数据传输速率。

① 无噪声时的信道容量公式为：

$$C=2F\log_2 N$$

其中，N 为每个码元所能携带的离散值的个数，即二进制数的位数。

② 有噪声时的信道容量公式为：

$$C=F\log_2\left(1+\frac{S}{N}\right)$$

其中，F 为信道带宽，单位为赫[兹](Hz)；S/N 为信噪比，单位为分贝(dB)；S 为信道上所传送信号的平均功率，单位为瓦[特](W)；N 为信道内部的噪声功率，单位为瓦[特](W)。在实际应用中信噪比一般表示为：$10\log(S/N)$，单位为分贝(dB)。

(13) 误码率：二进制码元在数据传输中被传错的概率。它是衡量系统可靠性的指标。它以接收信息中错误位数占总传输位数的比例来衡量。网络中要求误码率低于 10^{-6}。

(14) 传输效率是指原始数据量与整个传送数据的比率，数值上等于数据包中数据的长度与整个包长度的比值。

(15) 吞吐量指单位时间内整个网络能够处理的信息总量，单位是 Bps 或 bps。在单信道总线型网络里，

$$\text{吞吐量}=\text{信道容量}\times\text{传输速率}$$

其中，信道容量指信道上的最大的数据传输速率。

(16) 网络负荷量是指单位面积中数据在网络中的分布量，即数据在网络中的分布密度。

(17) 信道的传播延迟是指信号在信道中传播，从源端到达目的端所需要的时间。

以上基本概念中波特率、比特率、带宽以及误码率是数据通信和衡量网络性能的主要技术指标。

2.1.2　数据的传输形式

数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。要在两地间传输信息数据必须有传输信道，数据的发送与接收也必须有发送设备和接收设备。发送设备、传输信道和接收设备是数据通信系统的必要组成部分。

1. 数据通信系统的组成

数据通信系统是通过数据电路将分布在异地的数据终端设备与计算机系统连接起来，实现数据传输、交换、存储和处理的系统，如图 2-1 所示。

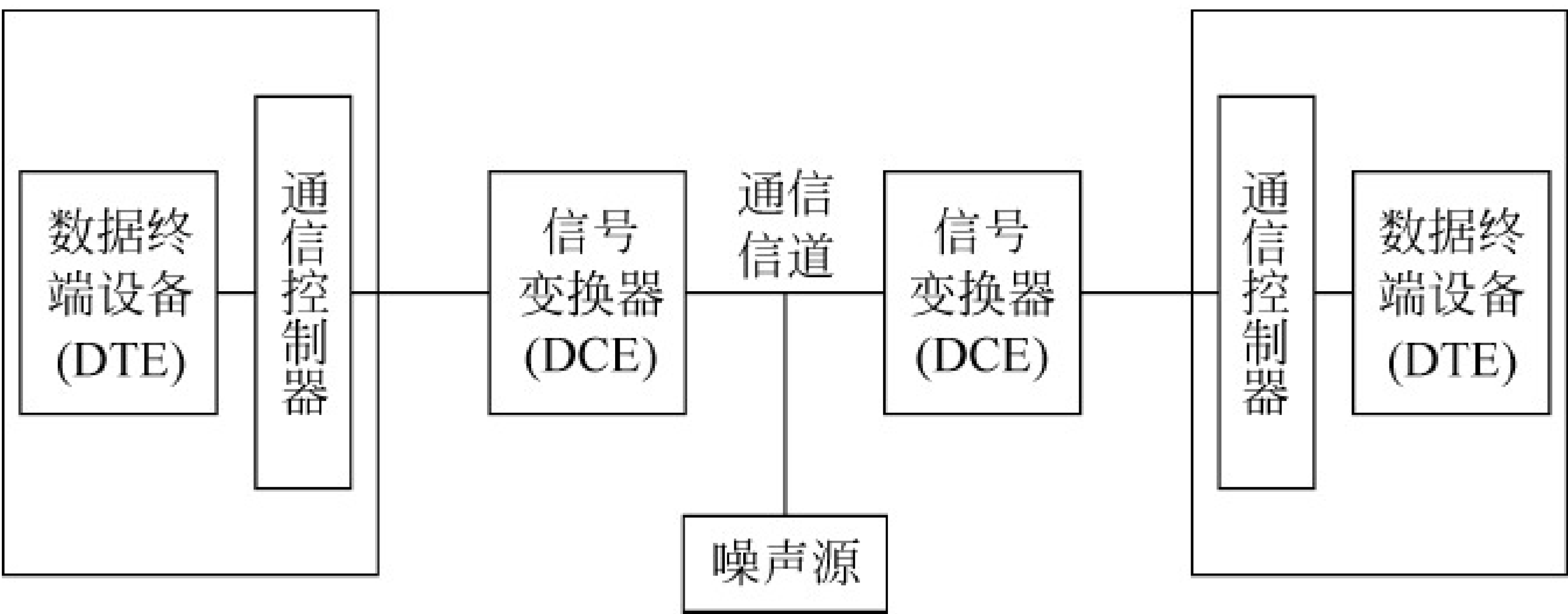


图 2-1 数据通信系统

从图 2-1 中可以看出,一个完整的数据通信系统一般由以下几部分组成。

(1) 数据终端设备(DTE)。在数据通信系统中,用于发送和接收数据的设备称为数据终端设备。最常见的数据终端设备就是计算机。另外,它还可以是网络中的某些专用数据输出设备,如打印机等。

(2) 通信控制器。该设备主要进行通信状态的连接、监控和拆除等操作,另外,它还可接收来自多个数据终端设备的信息,并进行信息格式的转换。如网卡就是通信控制器。

(3) 通信信道。它是数据在信号变换器之间传输所经过的通道,如电话线路、专用数字通信信道、CATV 电缆和光纤等。

(4) 信号变换器(DCE)。它的功能是把通信控制器提供的数据变换成适合在通信信道进行传输的信号形式,或者把信道中传来的信号变换成可供数据终端设备使用的数据,以保证传输质量,同时也为用户设备提供入网的连接点。最常见的信号变换器是调制解调器和光纤通信网中的光电转换器。

2. 数据通信的基本方式

通信所使用的信号分为模拟信号和数字信号,所以数据通信的方式也分为模拟数据通信和数字数据通信两种。

(1) 模拟数据通信

模拟数据通信用来传输模拟数据或数字数据对应的模拟信号。例如当前广泛使用的电话系统和电视系统就是典型的模拟数据通信。

模拟数据通信在实现远距离传输方面,一般不直接传输模拟信号,而是在发送方使用某一频率的电磁波作为载波,然后再用模拟信号或数字信号对其进行调制,调制后的载波信号(为模拟信号)占有以该载波频率为中心的一段频谱,并将其在适于该载波频率的介质上进行传输;而数据的接收方则通过解调将载波信号还原为原来的模拟信号或数字信号。

(2) 数字数据通信

数字数据通信是利用数字传输技术在数字设备之间传输数字数据或模拟数据对应的数字信号。由于计算机自身使用二进制的数字信号,所以计算机与其外部设备以及计算机局域网、城域网大多数直接采用数字数据进行通信。另外,目前北美采用的 24 路 PCM 脉码调制(速率为 1.544Mbps)电话系统,以及欧洲和我国采用的 30 路 PCM 脉码调制(速率为 2.048Mbps)电话系统都是数字数据通信系统。

数字数据通信传送的是数字信号，即逐位传送二进制数字，所以要求系统能明确知道传输线上正在传送的是 0 还是 1。

数字数据通信具有以下特点：

- 声音、视频和其他各类数据都可统一为数字信号的形式，并通过数字通信系统进行传输。
- 数字设备能较容易地通过集成电路来实现，并与计算机直接结合。目前由于超大规模集成电路技术的迅速发展，数字设备的集成度大大提高而成本却大幅下降，性价比很高。
- 在数据的传送中以帧为单位，并能通过检错编码和重发数据帧来发现与纠正通信当中的错误，保证了通信的可靠性。
- 使用加密技术可充分保证通信的安全性。
- 在远距离数字通信中可利用中继器放大和整型来保证数字信号的完整性。

3. 数据通信的方向

通信线路可由一个或多个信道组成，根据信道中某一时间信息传输的方向，可以分为单工通信、半双工通信和全双工通信三种方式。

（1）单工通信。信号只能向一个方向传输，任何时候都不能改变信号的传送方向，发送方不能接收，接收方也不能发送。信道的全部带宽都用于由发送方到接收方的数据传送。单工通信如图 2-2 所示。我们平时听广播和看电视就是单工通信，信息只能从广播电台和电视台发射并传输到各个家庭，但是不能实现反向传输。

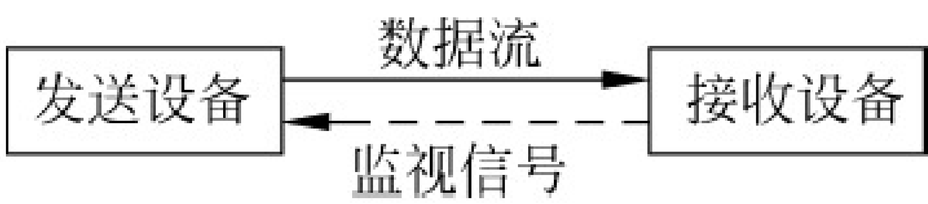


图 2-2　单工通信

（2）半双工通信。信号可以双向传送，但必须交替进行，即某一时刻只能向一个方向传输。半双工通信如图 2-3 所示。平时的对讲机就是这种方式。

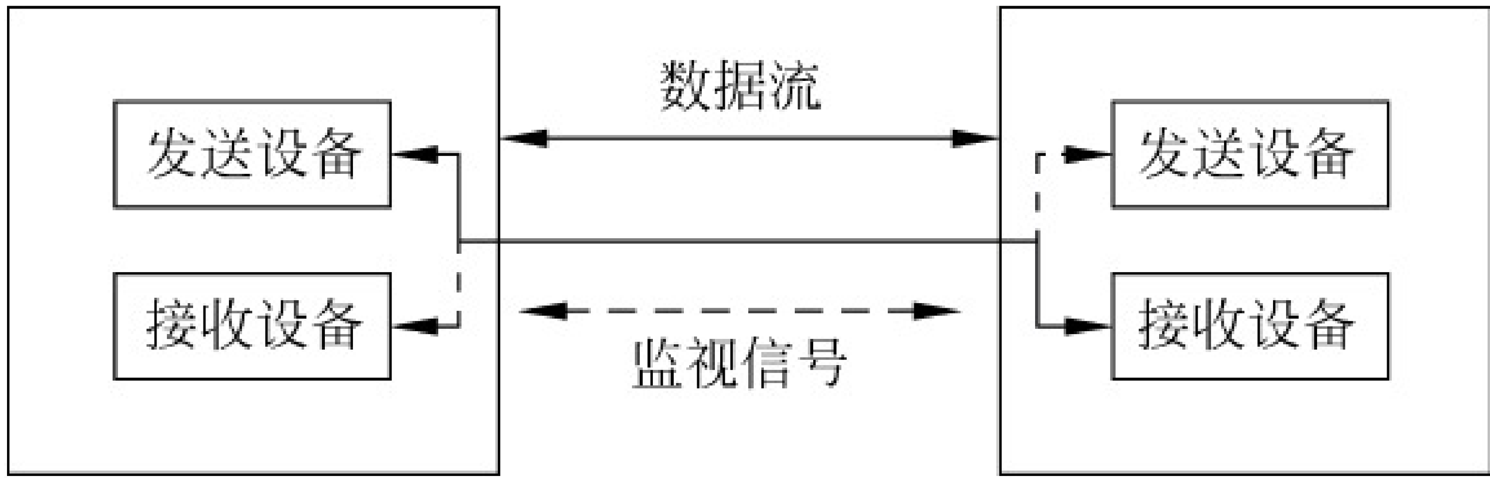


图 2-3　半双工通信

（3）全双工通信。信号可以双向同时传送。要求信道能够提供双向传输的双倍带宽。全双工通信如图 2-4 所示。例如计算机与计算机之间的通信。

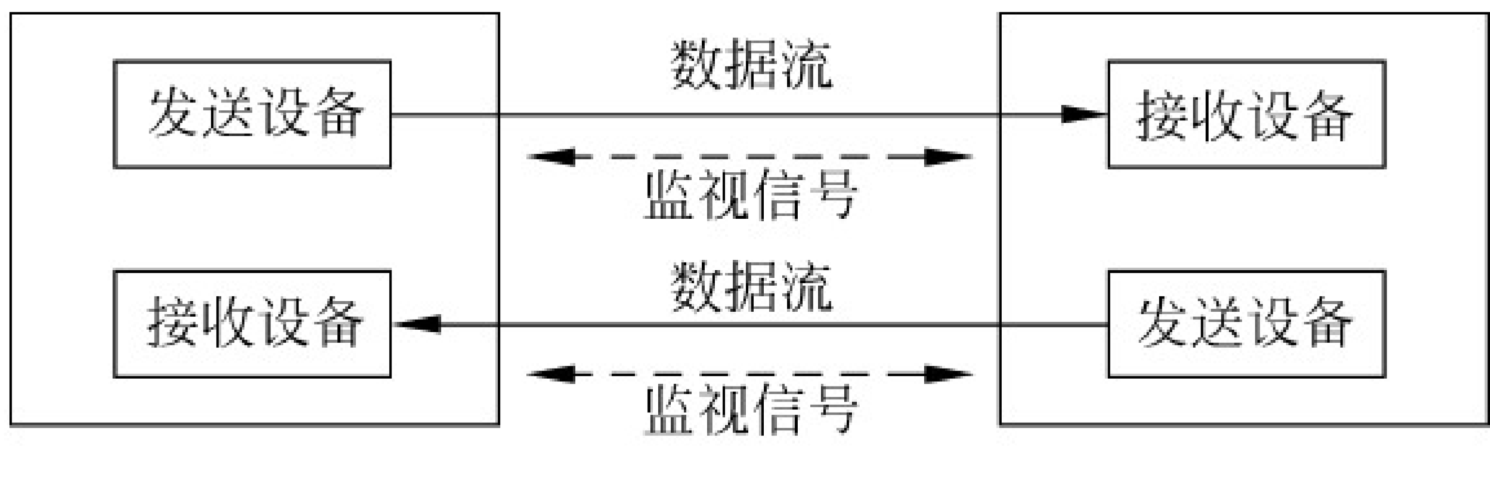


图 2-4　全双工通信

4. 基带传输与频带传输

(1) 基带传输

计算机中二进制比特序列的数字数据信号是典型的矩形脉冲信号。将矩形脉冲信号的固有频带称为基本频带,简称基带。

在数字通信信道上,直接传送基带信号(数字信号)的方法就是基带传输。基带传输一般用在较近距离的数据通信中,如在计算机局域网中。

(2) 频带传输

频带传输即用占据小范围带宽的模拟信号作为载波来传送数字信号,它是一种利用模拟信道传输数字信号的传输方式。

2.1.3 数据的传输介质

传输介质是组成信道的主要部分,信号的传输质量不仅与数据信号和收发特性有关,而且还与传输介质的特性密切相关。

传输介质的特性有以下几个方面。

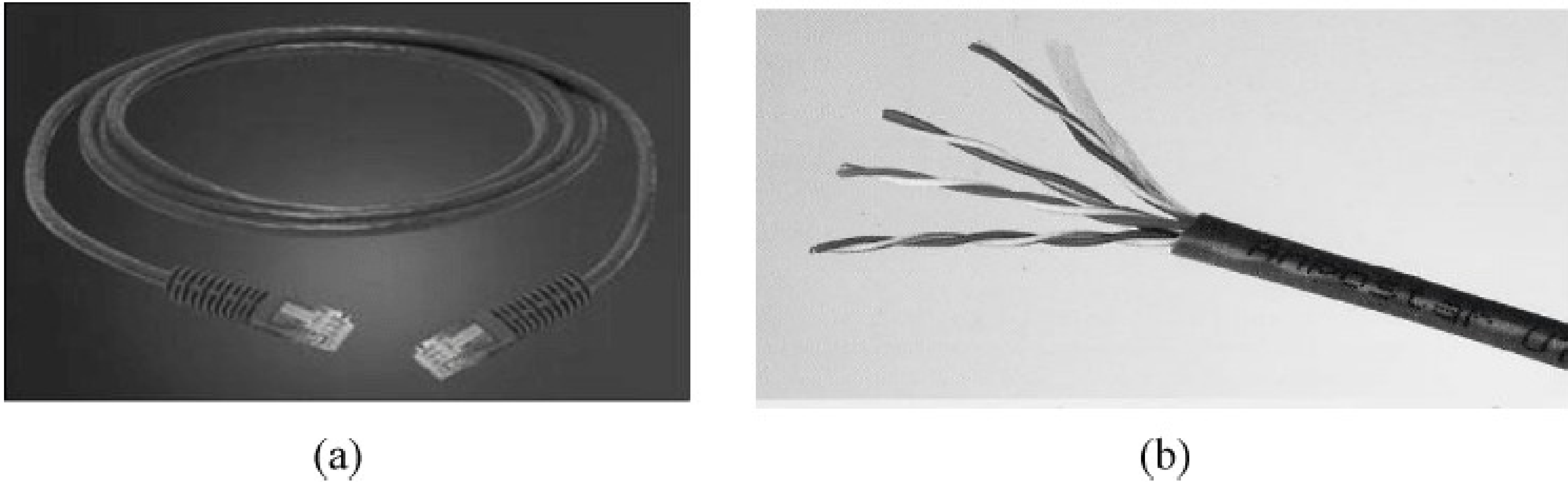
- 物理特性:它主要说明传输媒体的特性。
- 传输特性:它主要说明是使用模拟信号传输还是使用数字信号传输、调制技术、传输的容量和传输的频率范围。
- 地理范围:在不使用中间设备并将失真控制在允许范围内的情况下,整个网络所能传输的最大距离。
- 抗干扰性:防止噪声、电磁干扰对传输影响的能力。
- 连通性:使用点到点连接还是多点连接。
- 相对价格:元器件、安装和维护等方面的价格。

常用的传输介质包括双绞线、同轴电缆、光导纤维以及无线传输介质。

1. 有线传输媒体

(1) 双绞线

双绞线(Twisted Pair Cable)也称为双扭线,它价格便宜而且安装十分方便,是最常用的传输介质,但性能较光纤要差一些。双绞线是由一对绝缘铜线绞在一起形成的有规则的螺旋形线,采用扭绞结构是为了减少在一根导线流发射的能量对另一根导线的干扰,也有助于减少其他导线中的信号对这根导线的干扰。所以扭绞得越密,抗干扰就越强,性能也越好,但是价格就越高。双绞线的外形和结构如图 2-5 所示。



(a) (b)

图 2-5 双绞线

双绞线分为非屏蔽双绞线(Unshielded Twisted Pair,UTP)和屏蔽双绞线(Shielded Twisted Pair,STP)两大类。STP 外面有一圈保护层,可大大提高抗干扰能力,但成本较高。UTP 外面没有保护层,易受各种电信号的干扰,但成本较低。电话系统中使用的双绞线一般是一对,而计算机网络中使用的双绞线一般是四对。

双绞线的分类如下所示。

1 类线(UTP-1,Cat1):一对双绞线,用于模拟电话线和低速数字传输,这一类电缆没有固定的性能要求,不用于数据传输。在 UTP 中 1 类线是最低档次。

2 类线(UTP-2,Cat2):4 对双绞线,用于数字电话用户线、ISDN 和 T1 线路(1.544Mbps)等。

3 类线(UTP-3,Cat3):4 对双绞线,要求每英尺至少扭绞 3 次,用于 4Mbps 令牌环网、10Mbps 以太网及 ISDN 话音线路等,它是大多数电话系统的标准电缆。

4 类线(UTP-4,Cat4):4 对双绞线,要求每英尺至少扭绞 3 次,用于语音传输和 16Mbps 令牌环网和 10Mbps 大型以太网等。

5 类线(UTP-5,Cat5):4 对双绞线,要求每英寸至少扭绞 3 次,用于 16Mbps 以上令牌环网和 100Mbps 以太网等,还支持异步传输模式(ATM)。

超 5 类线(Cat 5e):它是 5 类线更高级别的版本。它包括高质量的铜线,提供高的缠绕率,并使用先进的方法以减少串扰。它能支持高达 200Mbps 的传输速率,是常规 5 类线容量的 2 倍,也是目前使用最多的一种电缆。

6 类线(UTP-6,Cat6):4 对双绞线,每对线由箔绝缘体包裹,所有的线对外层还有一层箔绝缘体包裹,箔绝缘体对串扰提供了较好的阻抗。Cat6 的吞吐量是 Cat5 的 6 倍。由于 Cat6 是一种新技术,且大部分网络技术还没有充分利用它的最高容量,所以,Cat6 很少用于当今的网络中。

STP(150Ω):用于 16Mbps 以上令牌环网、100Mbps 以上大型以太网及 600Mbps 以上的全息图像传输等。

在实际应用中最常用的 UTP 是 3 类线、5 类线。5 类线比 3 类线大大增加了单位长度内的绞合次数,5 类线在线对间的绞合度和线对内两根导线的绞合度都经过了严格的控制,使干扰在一定程度上可以相互抵消,从而大大提高了线路的传输特性。

现在普遍使用的高质量的 UTP 是在 2000 年作为标准正式颁布的称为超 5 类线 UTP(Cat 5e)。10Base-T、100Base-Tx 常用 5 类线或超 5 类线,但只使用了其中的两对线;100Base-T4 使用 3 类线的全部 4 对线;1000Base-T 使用超 5 类线的全部 4 对。

(2) 同轴电缆

同轴电缆是由一根空心的外圆柱形的导体围绕着单根内导体构成的。内导体为实芯或多芯硬质铜线电缆,外导体为硬金属或金属网。内外导体之间有绝缘材料隔离,外导体外还有外皮套或屏蔽物,如图 2-6 所示。

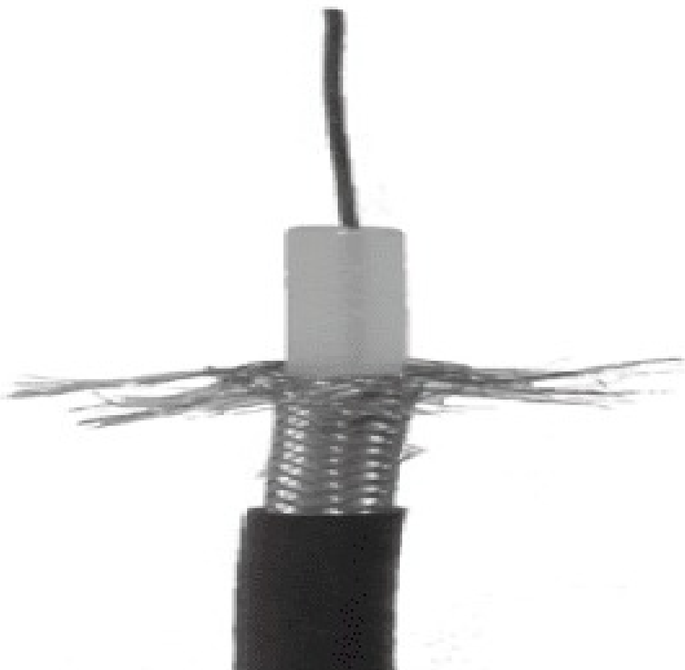


图 2-6 同轴电缆

同轴电缆可以用于长距离的电话网络、有线电视信号(CATV)的传输通道以及计算机局域网络。50Ω 的同轴电缆

可用于数字信号发送，称为基带；75Ω 的同轴电缆可用于频分多路转换的模拟信号发送，称为宽带。在抗干扰性方面，对于较高的频率，同轴电缆优于双绞线。

同轴电缆构造的网络现在已很少见了，因为网络中微小的变化，都可能会改动电缆。再者，这是一种总线结构，只要有一处连接出现故障，就会使整个网络陷入瘫痪，所以在双绞线以太网出现以后，这种传输介质基本上就不再被使用了，现在主要应用于有线电视信号的传输。

（3）光导纤维

光导纤维（简称光纤）是采用超纯的熔凝石英玻璃拉成的比人头发丝还细的芯线。一般的做法是在给定的频率下以光的出现和消失分别代表两个二进制数字，就像在电路中用通电和不通电来表示二进制数一样。光纤通信就是通过光纤传递光脉冲进行通信的，如图 2-7 所示。

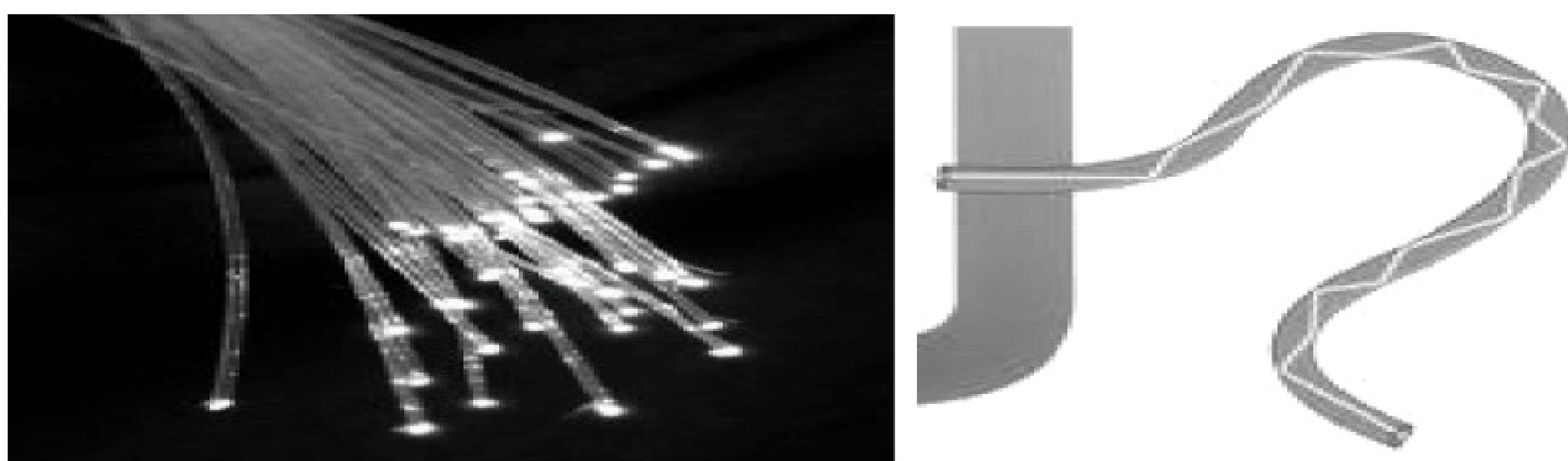


图 2-7 光导纤维

光纤导芯外面由一层折射率较低的玻璃同心层包裹，形成圆柱体，使光线全反射至导芯内，经过多次反射，达到传导光波的目的。每根光纤只能单向传送信号，因此，光缆中至少包括两条独立的导芯，一条发送，一条接收。一根光缆可以包括两根至数百根光纤，并用加强芯和填充物来提高其机械强度。

光纤可以分为单模光纤和多模光纤。所谓单模光纤是指直径小到只有单个波长的光纤，此种光纤形成了一种波导管，光线不需经过多次反射而是一直向前传播；而多模光纤是指可以传播多条光线的光纤，因为只要光线到达光纤表面的入射角大于临界角，就产生全反射，因此，只要入射角不同，多条光线可以在同一条光纤中传播。

在使用光纤的通信系统中采用两种不同的光源：发光二极管（LED）和注入式激光二极管（ILD）。发光二极管通电时会产生可见光，价格便宜，多模光纤采用此种光源。注入式激光二极管产生的激光定向性好，用于单模光纤，价格要昂贵得多。

光纤传输具有如下优点：

① 光纤的传输速率高，能超过千兆位/秒。

② 光纤传输频带非常宽，因而通信容量大。

③ 光纤的误码率极低，传输衰减小，无中继距离长，特别适合远距离传输。

④ 光纤无串音干扰和辐射，不易被窃听或截取数据，因而安全保密性好。

⑤ 光纤不受雷电和外界电磁波的干扰，适合在电气干扰严重的环境中应用。

⑥ 光纤的体积小，重量轻，成缆后弯曲性能较好。

但光纤也有缺点：光纤价格较贵，连接两根光纤时需要专用设备，施工要求精确高，

技术难度大，需要专业技术人员操作。另外，由于光的传输是单向的，双向传输需要两根光纤或一根光纤上的两个频段。

2．无线传输媒体

无线传输是利用空气等作为传输介质实现信号传播。

（1）无线电波通信

在一些电缆光纤难以通过或施工困难的场合，如高山、湖泊等，再如在老城区中开挖马路下设电缆有时也很不划算；尤其是在通信距离很远、对通信安全性要求又高、铺设电缆比较昂贵时，使用无线电波传输信号，就会比较灵活，使通信能轻松实现，而且抵抗自然灾害能力和可靠性都较高。

（2）微波通信

微波通信的载波频率为 2～40GHz。可同时传输大量信息。但微波是直线传播的，故在地面的传播距离有限，所覆盖的范围很大程度上依赖于天线的高度，天线越高，信号传输距离越远，所以常见的做法就是将天线安装在塔顶，而塔又建立在较高的山顶上。

（3）卫星通信

卫星通信是利用地球同步卫星作为中继站来转发微波信号的一种特殊微波通信形式，这时卫星作为一个超高天线和转发器。卫星通信可以克服地面微波通信距离的限制，三个同步卫星可以覆盖地球上的全部通信区域。

（4）红外通信和激光通信

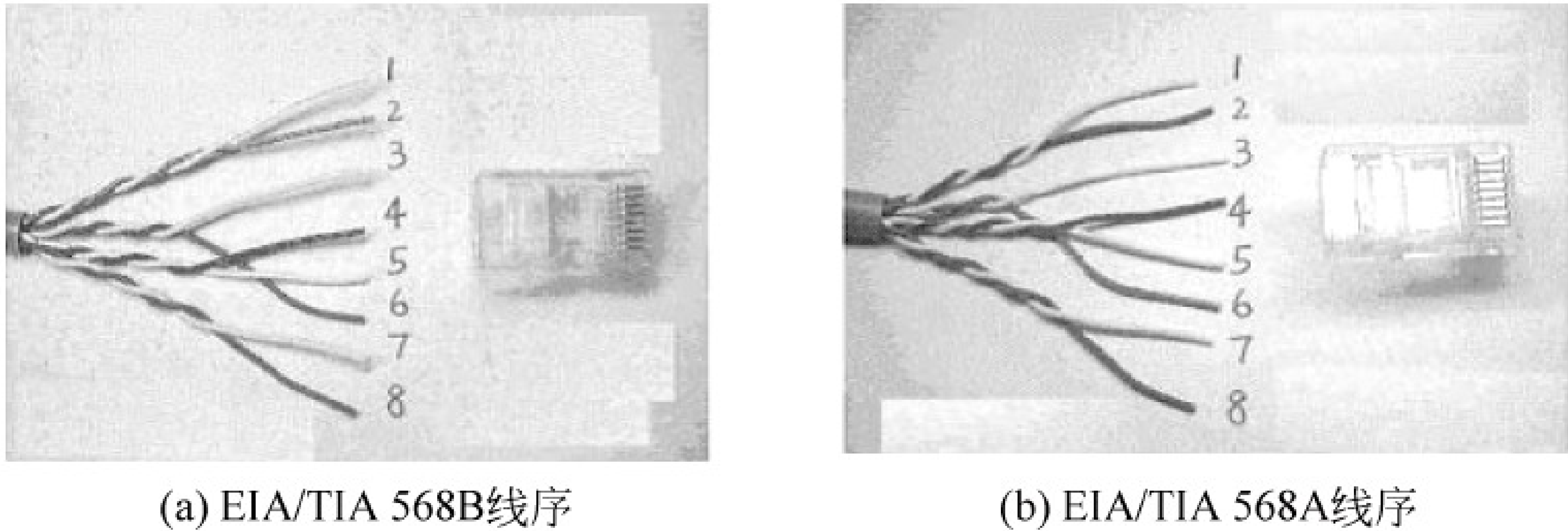
红外通信和激光通信有很强的方向性，都是沿直线传播的。红外通信和激光通信要把传输的信号分别转换为红外信号和激光信号后才能自由地在空间沿直线传播，它们难以被窃听、插入数据和干扰，但是它们对雨雾环境比较敏感。

任务完成：双绞线的制作。

在制作网线时，要用到 RJ-45 接头，俗称“水晶头”的连接头，如图 2-8 所示。在将网线插入水晶头前，要对 8 条线排序。根据 EIA/TIA 接线标准，RJ-45 接口制作有两种排序标准：EIA/TIA 568B 标准和 EIA/TIA 568A 标准。8 条线根据颜色从上到下排列顺序如图 2-8 所示。

EIA/TIA 568B 标准的线序为：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕（图 2-8(a)）。

EIA/TIA 568A 标准的线序为：白绿、绿、白橙、蓝、白蓝、橙、白棕、棕（图 2-8(b)）。



(a) EIA/TIA 568B线序　　(b) EIA/TIA 568A线序

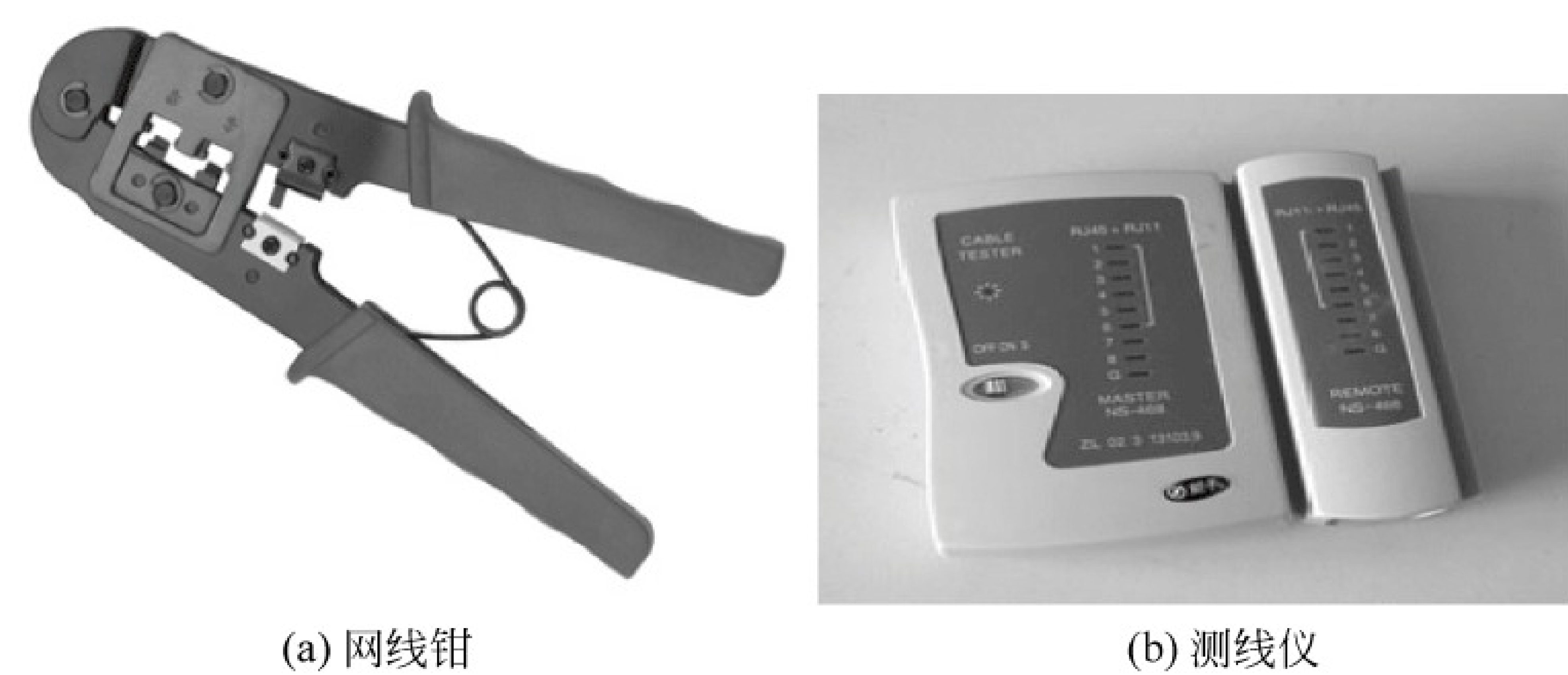
图 2-8　EIA/TIA 线序标准

另外，根据双绞线两端线序的不同，有两种不同的连接法：直接连接法和交叉连接法。

直接连接法是线缆的两端使用同一种线序。直接连接法通常用于不同类型的设备的相互连接。如计算机连接集线器、计算机连接交换机等。

交叉连接法是线缆的两端使用不同的线序。这种排序用于连接同种设备，如两台计算机之间直接相连。这里用到的就是交叉双绞线。

制作双绞线通常要用到两种工具：网线钳和测线仪（如图 2-9 所示）。



(a) 网线钳　　(b) 测线仪

图 2-9　网线钳和测线仪

双绞线制作过程如下：

① 用网线钳将网线两端的表皮（长度为 13～15mm）剥去，按前面介绍的线序为网线排序。

② 将排好序的网线并拢，注意并拢时不要使线序发生变化。

③ 将排好序的网线剪齐（留下约 12mm）。

④ 将网线插入水晶头，注意插入时使水晶头有金属片的一端对着自己。

⑤ 将网线插入水晶头后，将水晶头放入网线钳的压线槽中，合拢钳子，将其压紧。

这样，网线也就制作好了。网线制作好后，需要用测线仪测试是否连通。测试的方法是将制作好的网线的两端插入测线仪的接口，打开电源开关后观察指示灯是否按顺序点亮：若 8 条线对应的灯都按顺序点亮，说明网线已连通；若有哪个灯不亮，则此条线不通。

任务 22　利用示波器查看数据传输的信号

任务描述：通过波形可以形象地理解电信号的传输，因为示波器可以根据信号参数的不同，生成不同波形。通过示波器来观察各种信号的波形形状，加深对信号编码与调制的理解。

2.2.1　数据到信号的编码

1. 数据的调制技术

不论是传输模拟数据还是数字数据，原始的数据经过调制就变成模拟信号通过相关的传输介质发送出去，在到达接收端后进行解调，再变换成原来的形式。所以我们先来了

解两个基本的概念：调制和解调。

调制是在发送端将数据放到正弦波上转换为模拟信号的过程。经过调制的信号可以在模拟信道上传输，它通过调制器完成。

解调是在接收端把接收到的模拟信号还原成原来信号的过程。它通过解调器完成。

载波信号主要包含了振幅、频率和相位三个重要的参数，所以所有的调制技术都涉及这三个参数中一个或几个的变化。

（1）模拟数据调制为模拟信号

模拟数据由模拟信号传输时不需进行变换，但是它要在高频下进行调制，输出信号也是一种频率极高的模拟信号。最常用的两种调制技术分别是幅度调制（AM）和频率调制（FM）。

① 幅度调制技术中，载波的幅度会随着原始模拟数据幅度变化而变化。调制过程中只是改变了载波的幅度而频率没有发生改变（如图 2-10 所示）。

② 频率调制技术中，高频载波的频率随着原始模拟信号频率的变化而变化。频率调制过程如图 2-11 所示，此调制过程中，载波频率会发生波动，而载波的幅度是不变的。

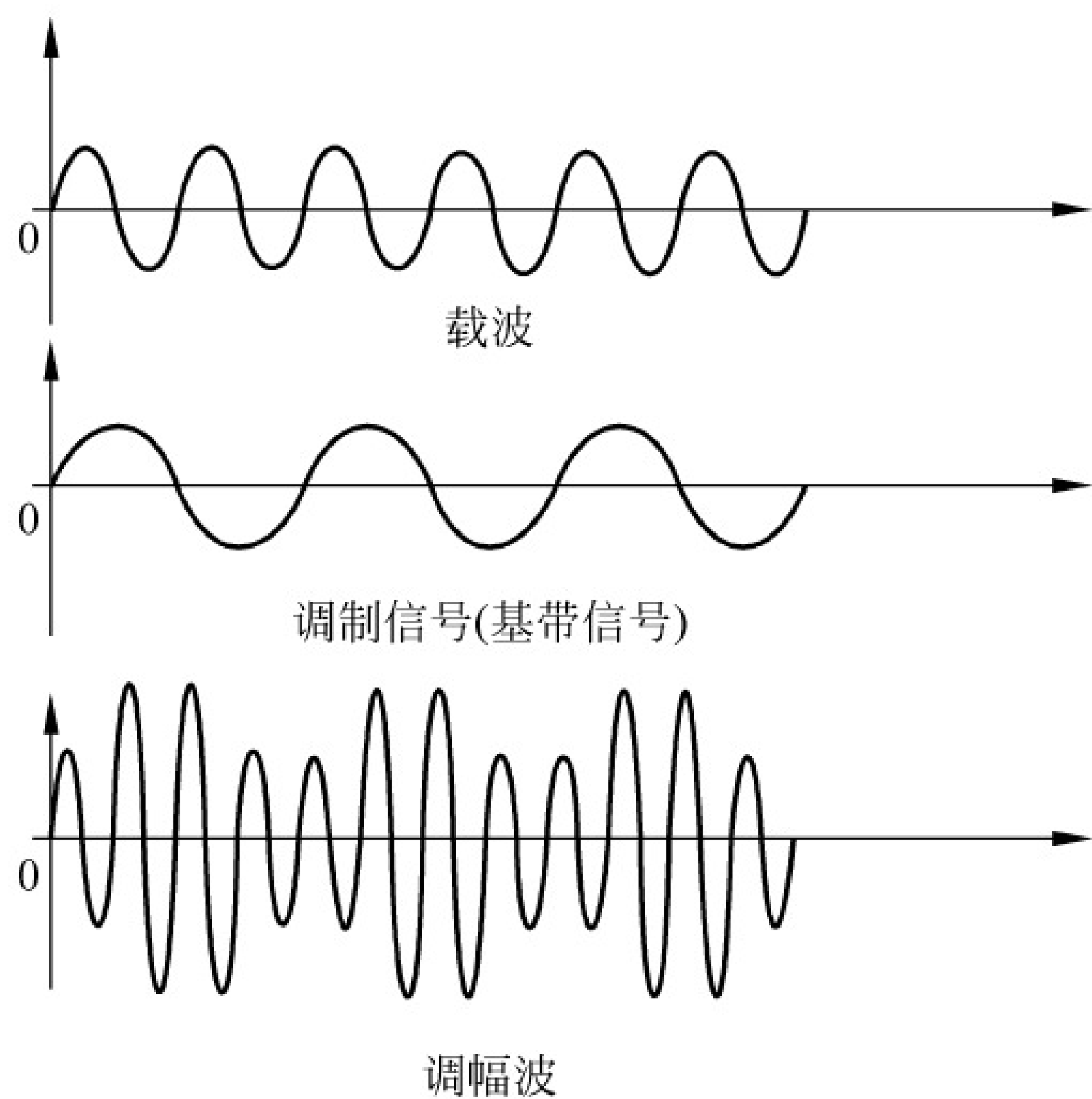


图 2-10　幅度调制

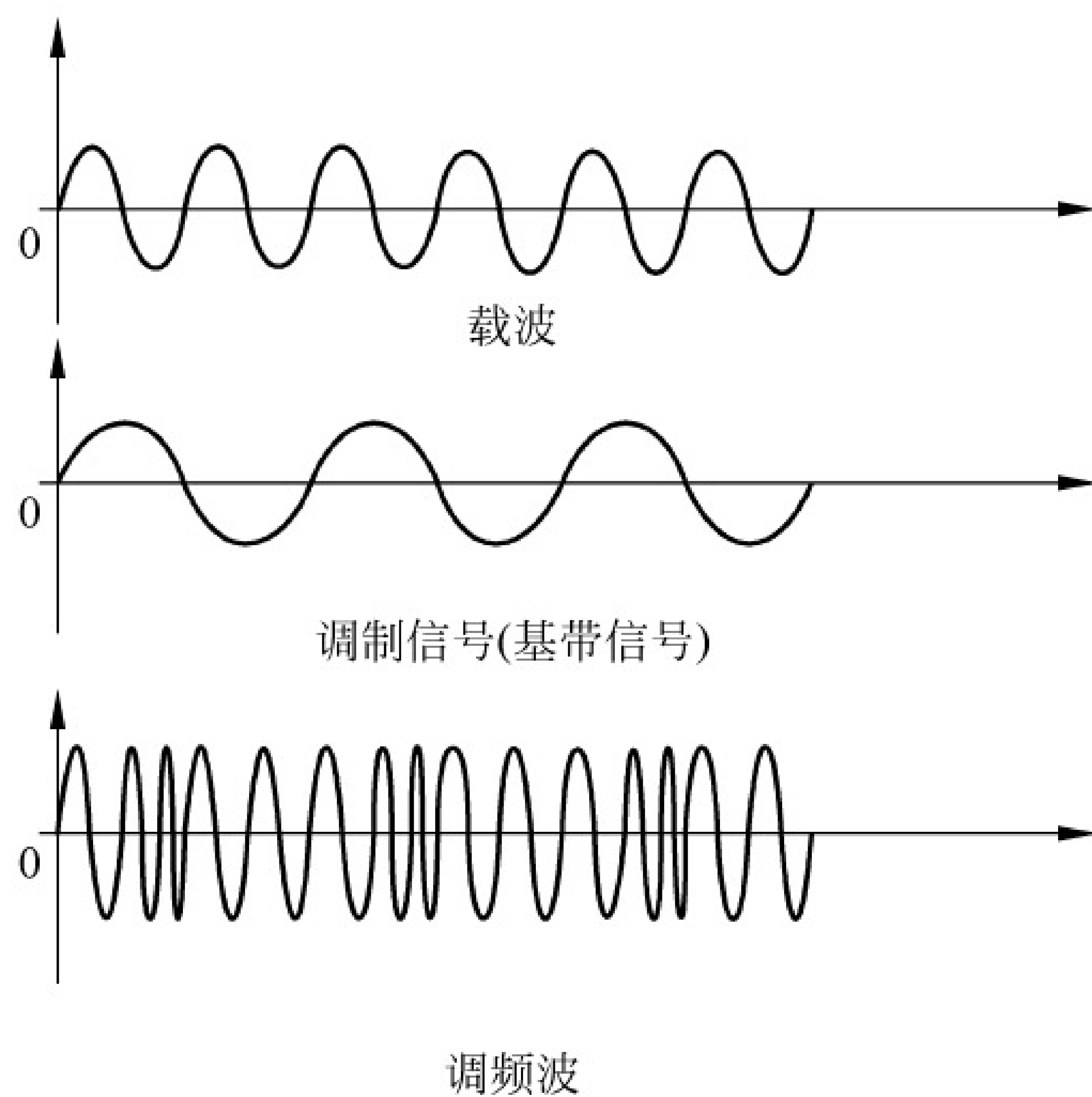


图 2-11　频率调制

（2）数字数据调制为模拟信号

该调制过程也是围绕着振幅、频率和相位这三个载波信号的特性进行的，所以分为三种调制方式：幅移键控法（ASK）、频移键控法（FSK）和相移键控法（PSK），如图 2-12 所示。

① 幅移键控法（Amplitude-Shift Keying，ASK）是通过改变载波信号的振幅来表示数字信号的“0”和“1”。有幅度值表示“1”，无幅度值表示“0”，波形的频率和初始相位不变。它实现简单，但是抗干扰性能差，在音频线路上一般只能达到 1200bps。

② 频移键控法（Frequency-Shift Keying，FSK）是通过改变载波信号的频率来表示数字信号的“0”和“1”。用高频率表示“1”，低频率表示“0”。它的抗干扰能力强，但是占用较宽的带宽。

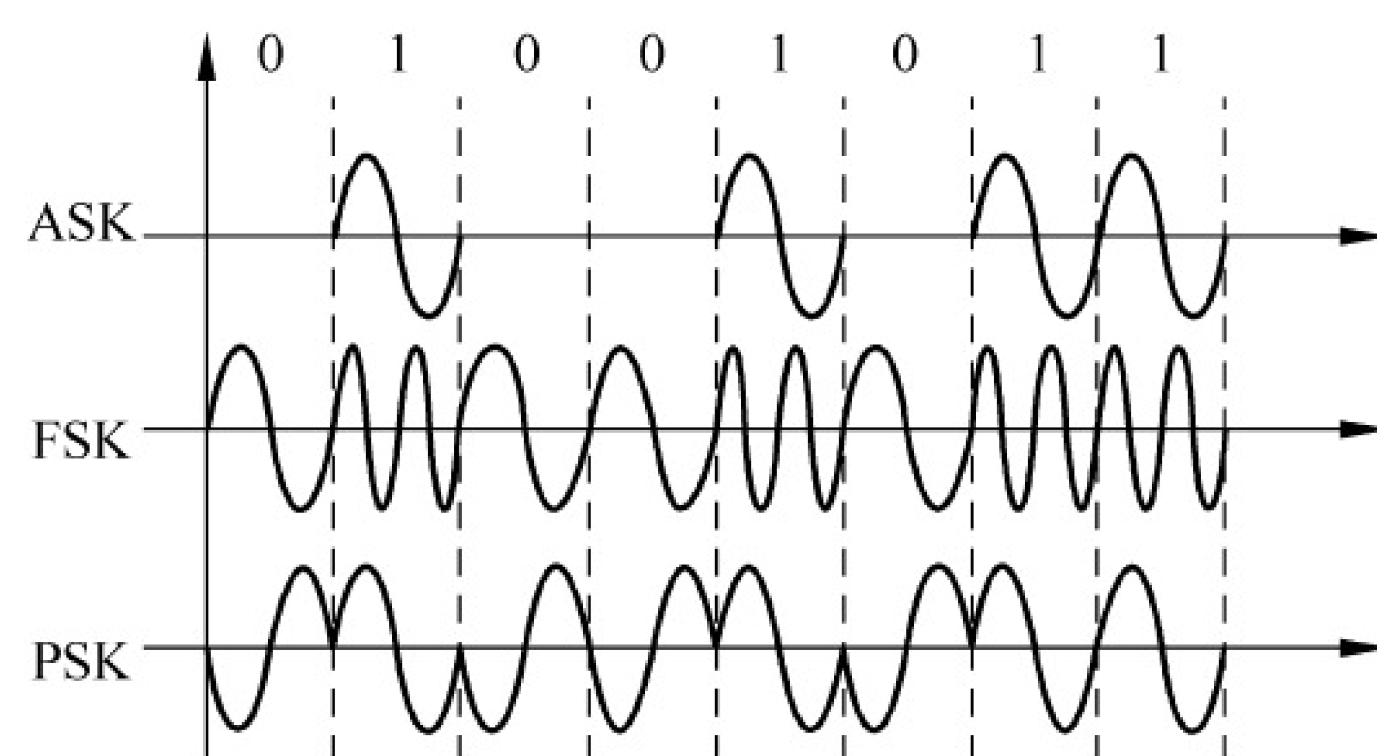


图 2-12　数字数据的模拟信号调制

③ 相移键控法(Phase-Shift Keying,PSK)是通过改变载波的初始相位来表示数字信号的“0”和“1”,波形的幅度和频率不变。用相位的绝对值来表示“0”和“1”。正弦波初始相位 0 表示“0”,初始相位 π 表示“1”。

调相方式为了提高调制速率也可以用一个正弦波形表示两位数据(四相调相),也可以采用幅度—相位复合调制。PSK 技术也具有较强的抗干扰性,而且比 FSK 方式更有效。在音频线路上,传输速率可以达到 9600bps。

2. 数据的编码技术

调制技术是把数据调制成模拟信号进行传输,而编码技术是将数据变换为数字信号,其中也有两个基本概念:编码和解码。编码是将模拟数据或数字数据变换成数字信号。解码指在接收端将数字信号变换成原来的形式。

(1) 数字数据编码为数字信号

数字信号其实就是用两个电平来表示两个二进制数字。无电压(也就是无电流)用来表示“0”,而恒定的正电压用来表示“1”。常见的数字数据的数字信号编码有以下几种。

① 双极性不归零码(BNRZ),如图 2-13(a)所示。相应的编码规则是在每一码元时间间隔内,发正电流表示“1”,发负电流表示“0”。正的幅度值和负的幅度值相等,所以被称为双极性码。它的判决门限定为零电平,接收信号的值在零电平以上,判为“1”;在零电平以下,判为“0”。

② 曼彻斯特编码,如图 2-13(b)所示。相应的编码规则是在每一码元时间间隔内,当传送“0”时,电平从低向高跳变;当传送“1”时,电平从高向低跳变。每一位的中间都有一次电平的跳变。该编码技术的优点是不包含直流分量,本身跳变可作为同步时钟使用。

③ 差分曼彻斯特码,如图 2-13(c)所示。相应的编码规则是在每一码元时间间隔内,用每位开始处有无跳变表示数据,开始有跳变表示“0”,开始无跳变表示“1”。每位中间的跳变只作为同步时钟,不代表数据。该编码技术的缺点是编码效率低。

(2) 模拟数据编码为数字信号

由于数字信号抗干扰能力强,所以有时需要将模拟信号数字化后再传输。在模拟数据的数字信号编码技术中,可以用一系列数字化脉冲信号(0 或 1)来表示模拟数据的信息。需要解决的问题是如何在不损失信号意义和质量的前提下,将信息从无穷多的连续值转换为有限个离散值。通常在发送端进行模/数(A/D)转换,一般将 A/D 转换器称为

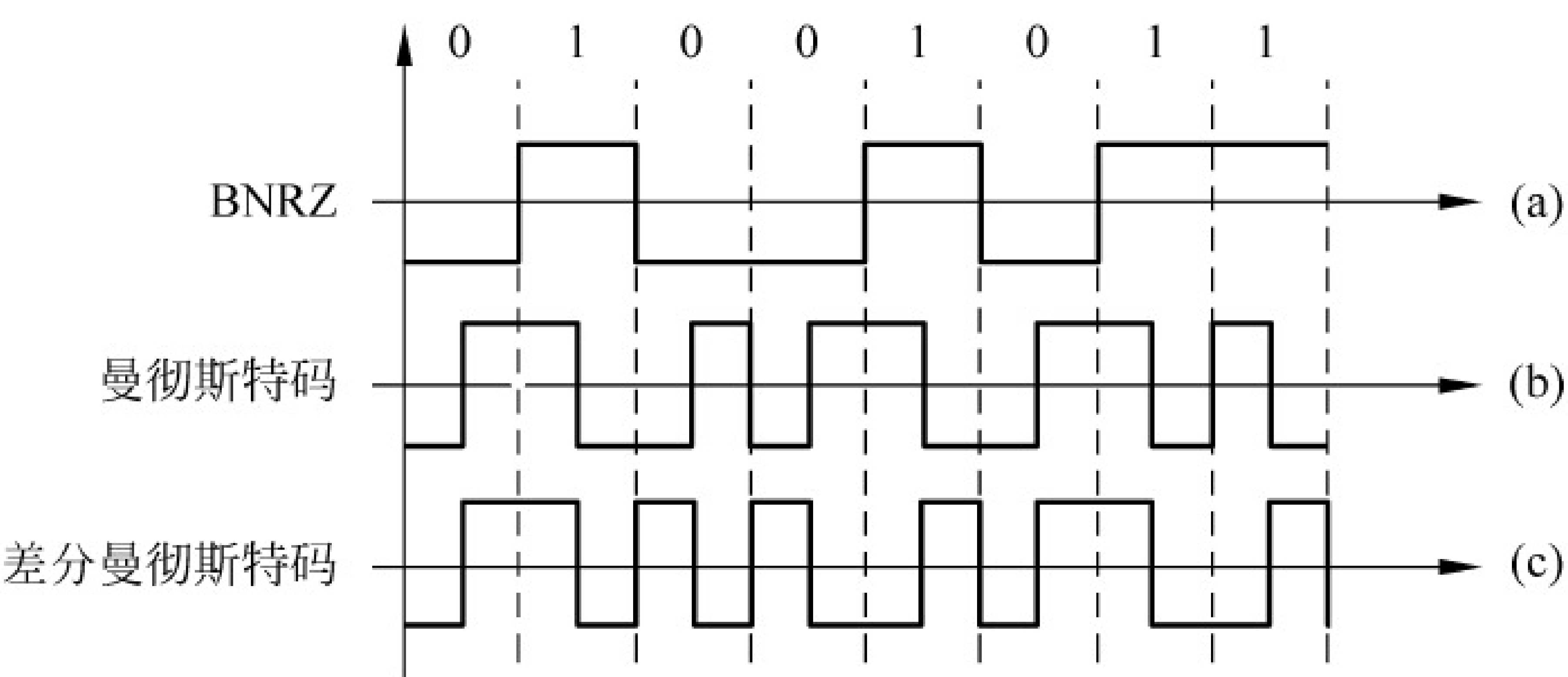


图 2-13　数字数据的数字信号编码

编码器；而在接收端进行数/模(D/A)转换，一般将 D/A 转换器称为解码器。

将模拟信号变换为数字信号的常用方法是脉冲编码调制(Pulse Code Modulation，PCM)，简称脉码调制。脉码调制以采样定理为基础，其编码过程包括采样、量化和编码三步，如图 2-14 所示。

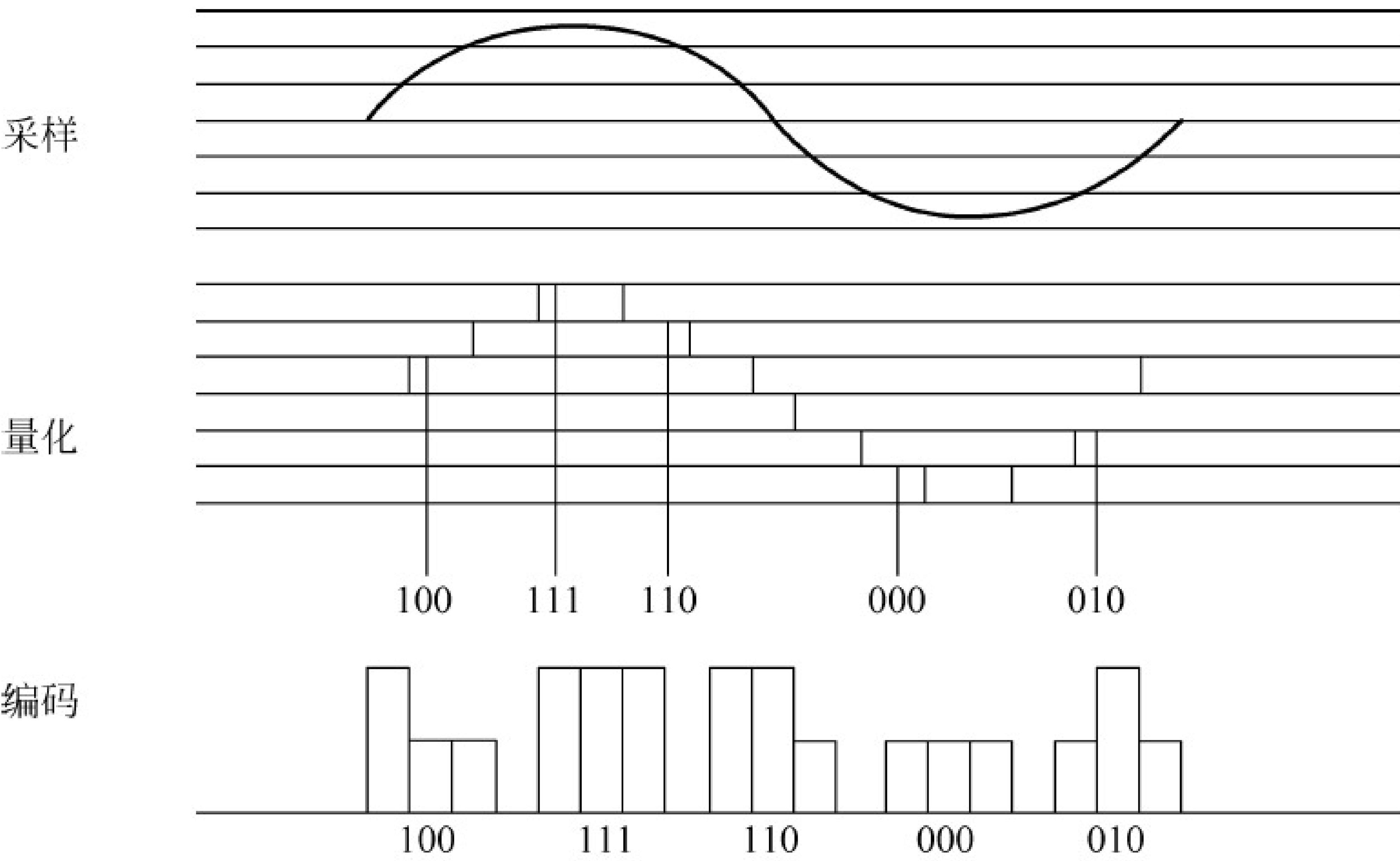


图 2-14　脉冲编码调制

采样：每隔一定的时间对连续模拟信号采样，采样得到的信号就成为一组离散的脉冲信号序列(PAM)。

量化：这是一个分级过程，把采样所得到的 PAM 脉冲按量级进行比较并且“取整”，此时脉冲序列就成为数字信号。

编码：用以表示采样序列量化后的量化幅度，它用一定位数的二进制码表示。

2.2.2　数据的传输过程

1. 数据传输技术

(1) 数据传输方式

将信息编码成可以传输的格式后，就要考虑数据的传输方式了。数据传送有两种方式：并行传输方式和串行传输方式。一般并行传输用于计算机内部各部件之间或近距离

设备之间的数据传输，而串行传输一般用于计算机与计算机或计算机与终端之间远距离的数据传输。并行传输一般是通过计算机的并行接口(LTP)进行的，而串行传输一般通过计算机的串行接口(COM)进行的(如图 2-15 所示)。

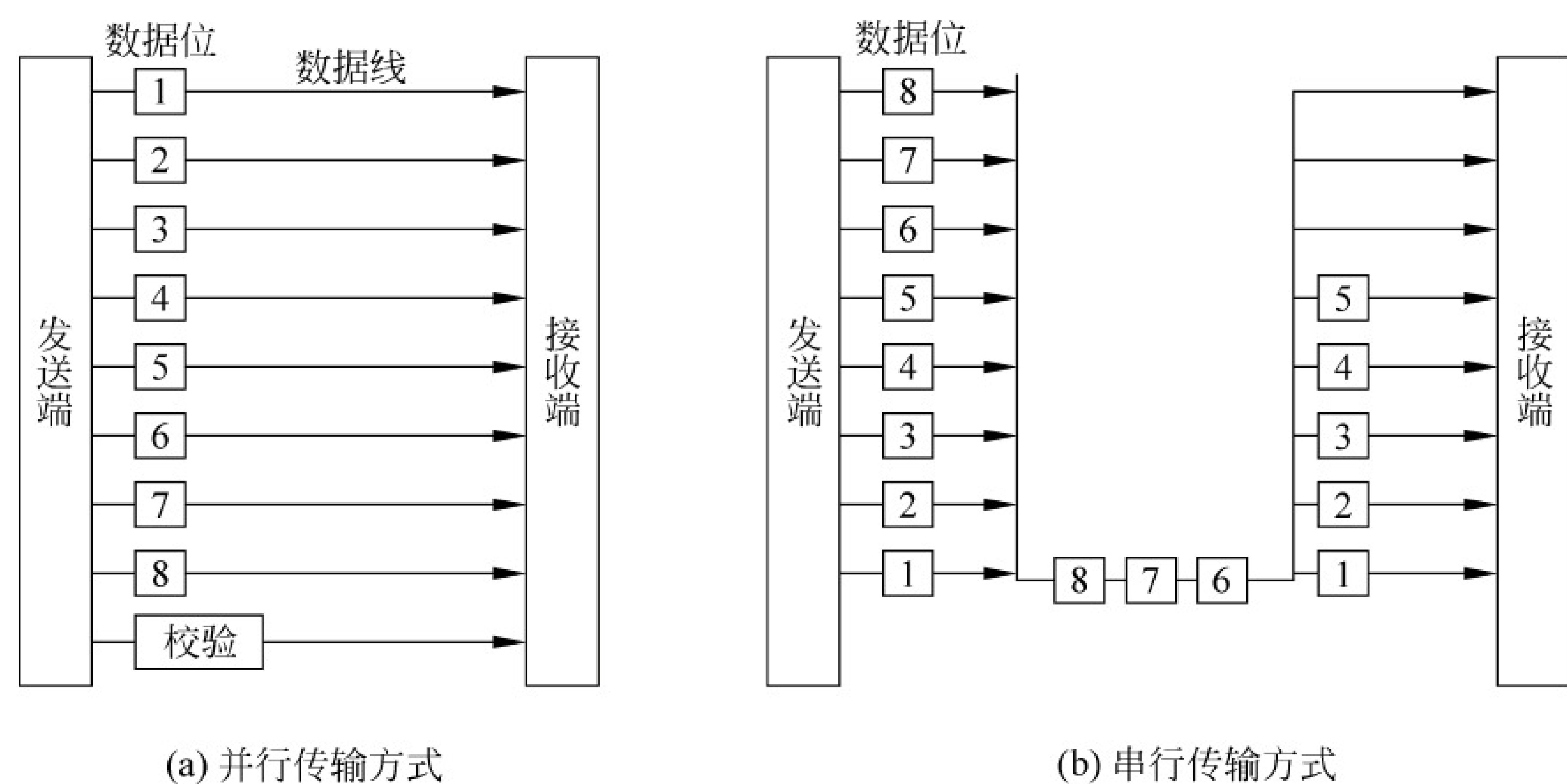


图 2-15　并行/串行传输方式

① 并行传输

一次同时将待传送信号经由 $n(n>1)$ 个通信信道同时发送出去。它以字符(8 个二进制位)为单位，一次传输一个字节的信号，所以传输信道需要 8 根数据线，同时还需要其他的控制信号线。由于并行传输一次只传输一个字符，所以收发双方没有字符同步的问题。

并行传输的优点是速度快，适应于短距离通信。缺点是费用高，维修不易，易受干扰。

② 串行传输

它是数据一位一位地传输，从发送端到接收端只需要一个通信信道，经由该通信信道逐位地将待传送信号的每个二进制代码依次发送。它适用于远距离的数据传输。

由于计算机内部操作大多使用并行传输方式，因此，当数据通信采用串行传输方式时，发送端需要通过并/串转换装置将并行数据位流变为串行数据位流，然后送到信道上传输，在接收端再通过串/并转换还原成 8 位并行数据流。

(2) 数据同步的方式

无论是并行传输还是串行传输，必须要解决的问题是数据发送方发出数据后，接收方如何在合适的时间正确地接收数据。也就是说从发送方连续不断送来的数据中，正确地区分出每一个代码，使收发两端保持同步(同步是指接收端要按发送端所发送的每个码元的重复频率和起止时间接收数据)，以便完成传输任务。

常用的数据同步方式有两种：同步传输方式和异步传输方式。这两种传输方式的区别在于发送和接收设备的时钟是异步的，还是同步的。

① 同步传输

同步传输方式传输时是将一个大的数据块(一组数据或一个报文)一起发送的。同步传输时，首先在传输的数据块前面放上两个或两个以上的同步信号字符 SYN(ASCII 代码为 0010110)，再在数据块结束后加上同步信号。接收端接收时，首先寻找同步字符

SYN,如果检出两个或两个以上的 SYN,那么后面的就是传输的字符,直至收到同步信号为止。数据块和前后的同步信号一起构成了一个数据单位,称为帧。

因为同步传输以数据块的方式传送,所以线路利用率高,而且它不需要起始位、停止位,中间不留空格也不用停顿,可连续发送,多用于字符信息块的高速传输。一般在发送几千比特之后需要再进行一次同步。但这种方式收发双方控制较为复杂,需要精度较高的时钟装置来协调,对线路的要求也高。并行传输一般都是同步传输,如计算机和打印机之间的通信使用的并口,采用的就是同步传输方式。

② 异步传输

异步传输方式就像使用键盘输入字符到主机一样,它允许码字之间存在不确定的空闲时间。异步传输也叫做起止式传输,它以字符为单位,在每个字符(8 比特)代码前增加一个起始位(逻辑“0”),字符代码后增加 1 位、1.5 位或 2 位停止位(逻辑“1”)。字符可以是 5 位或 8 位,一般来说,5 位字符的停止位是 1.5 位,而 8 位字符的停止位是 2 位。

在异步传输方式中,由于每个字符都带有起始位和停止位,所以可随时发送字符。当没有数据发送时,传输线一直处于高电平状态(停止位/逻辑“1”),一旦接收端检测到传输线上由“1”到“0”的跳变,意味着发送端已开始发送字符。这时接收端利用这个电平从高到低的跳变启动定时机制,按发送的速率顺序接收字符;一个字符发送结束,发送端又使传输线处于高电平,直到发送下一个字符为止。由于每个字符是独立传输的,为了防止发送端和接收端发生时钟漂移,要求它们的时钟必须同步,但由于一次只接收一个字符,对接收端时钟的精度要求就降低了。

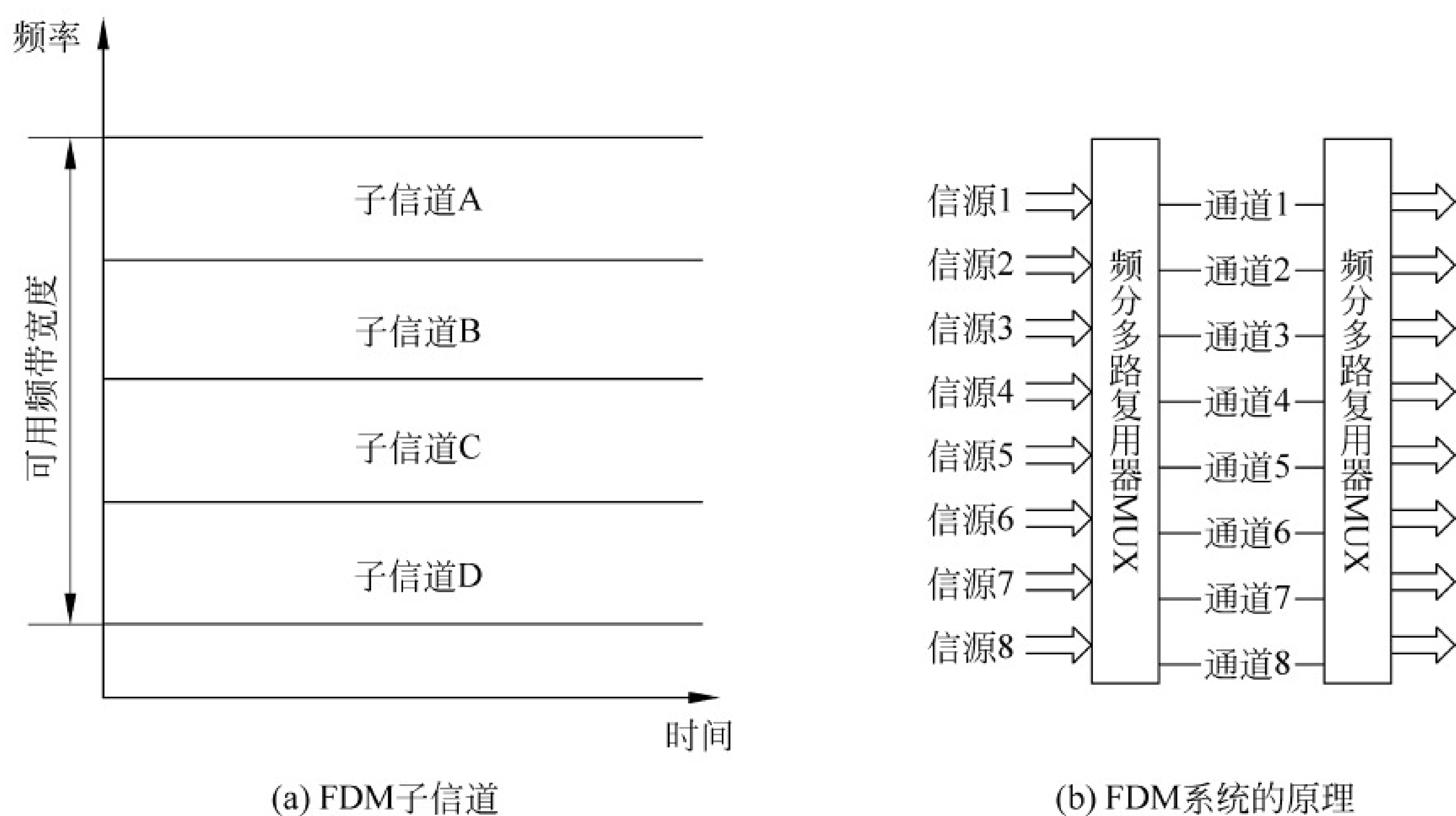
同步传输效率高于异步传输,但是线路控制比较复杂,要有发送检测同步字符的线路。如果时钟失步了,会破坏整个数据块的正确性。而异步传输以串行方式发送并附有起止位,字符间通过空号(高电平)分割,设备简单,技术容易,费用不高,但是速率较低。即使有一次时钟失步了,也只影响这一个字符的正确接收。

2. 多路复用技术

多路复用技术是指在同一个物理信道上同时传输多路信号,实现通信信道共享的一套技术。被传输的多路信号可以由不同的信源产生,传输信号时各路信号之间互不影响。因此,它提高了传输介质的利用率。常用的多路复用技术有:频分多路复用(FDM)、时分多路复用(TDM)和波分多路复用(WDM)等。

(1) 频分多路复用技术

频分多路复用技术(Frequency Division Multiplexing,FDM)主要是利用了传输介质的带宽优势,当传输介质的有效带宽远远超过被传输的信号带宽时,就可以把多个信号调制在不同的载波频率上,从而在同一介质上实现多路信号并行传输,即将信道的可用频带(带宽)按照频率不同分成多个互不重叠的频段,每个信号占据其中一个频段,从而能开辟出多个子信道,各通道之间用保护频带进行隔离,以保证各路信号的频带不会发生重叠(如图 2-16(a)所示)。到达接收端后,用适当的滤波器将多路信号分离,再分别进行解调和终端处理。它的输入信号可以是模拟的,也可以是数字的。如电话、有线电视、非对称用户数字线(ADSL)都利用了该技术进行信息传输,电话系统中利用它可以同时传输 24 路信号。FDM 系统的原理如图 2-16(b)所示。



(a) FDM子信道　　(b) FDM系统的原理

图 2-16　频分多路复用技术

频分多路复用技术的优点是信道的利用率极高，允许复用的路数较多，分路也非常方便，并且频度越大，它能容纳的用户数就越多。缺点是设备比较复杂，不仅需要大量的调制器、解调器和滤波器，而且在接收端还要提供相关载波。另外，由于在传输过程中的非线性失真及频分复用信号抗干扰性能差，不可避免地会产生路际串音干扰。所以一般情况下，都采用多级调制的方法。

（2）时分多路复用技术

时分多路复用技术（Time Division Multiplexing，TDM）是利用了传输介质的高传输速率的优势，如果传输介质的传输速率远超过单一信源要求的数据传输速率，就可以将一条线路按工作时间先划分周期，每一周期再进一步划分成若干时间片 t_1，t_2，t_3，…，t_n，再将时间片轮流分配给多个信源来使用，在每个周期的每个时间片 t_i 内，线路只提供给一对终端使用。也可以来这样理解 TDM，假如在一个饭店内同时有 10 桌人吃饭，饭店在处理时并不是先把第一桌的菜全部做好上齐后，然后再做第二桌菜；第二桌全做好后再做第三桌……而是轮流给各桌先上第一道菜，然后回来再轮流给各桌上第二道菜、第三道菜……依次进行，直到把所有的菜全部上完。时分多路复用原理如图 2-17 所示。

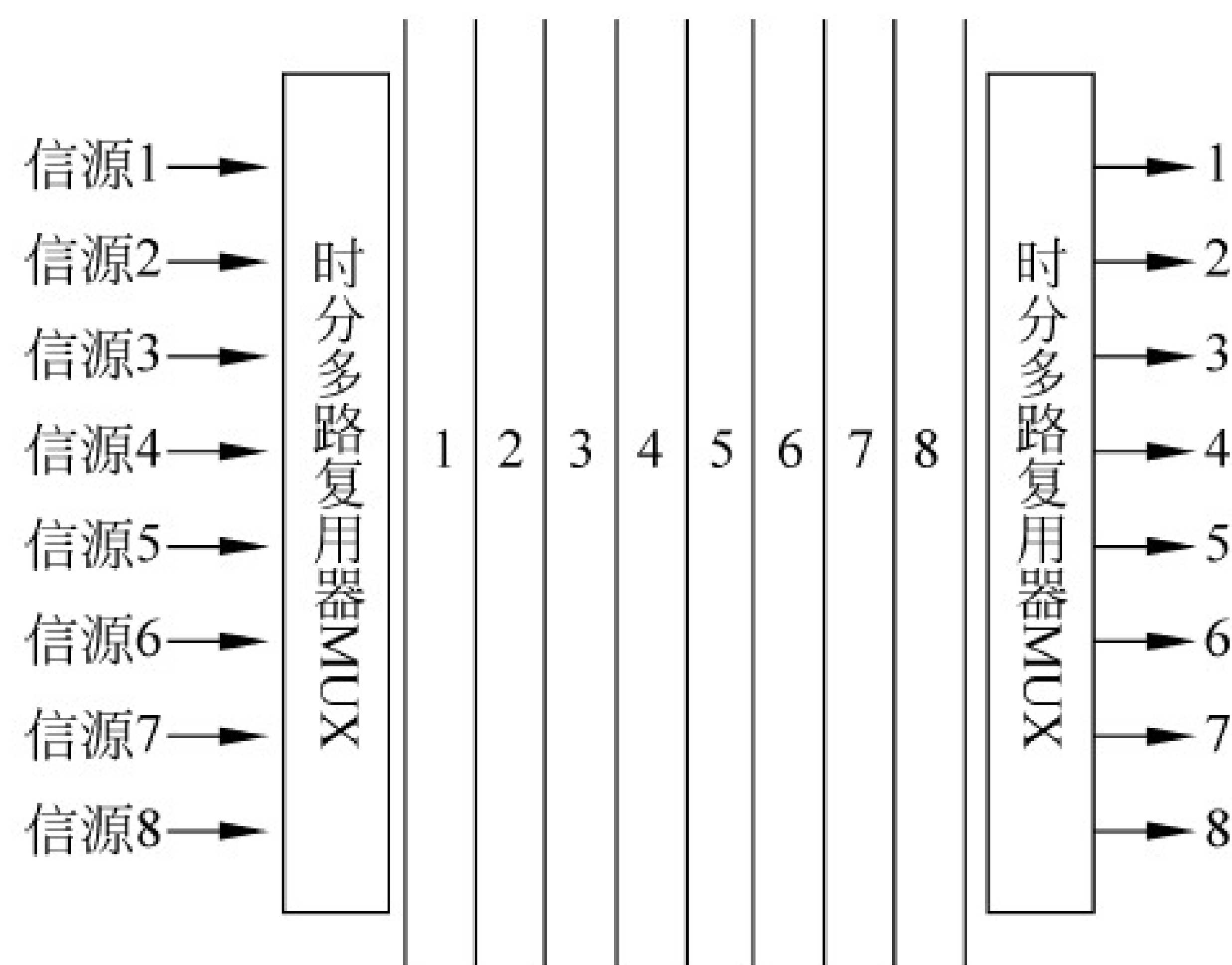


图 2-17　时分多路复用原理

TDM 又有两种实现方式：同步时分多路复用（Synchronous Time-division Multiplexing）和异步时分多路复用（Asynchronous Time-division Multiplexing）。同步时分多路复用中的“同步”和同步传输技术中的“同步”不同，这里是指按照固定顺序，把时间片循环轮流地分配给各路信号，而不管某路信号是否需要继续发送数据或数据已发送完成，所以它容易造成信道资源的浪费。

异步时分多路复用也称为统计时分复用(Statistical TDM,STDM)。同样这里的“异步”与异步传输中的“异步”也不同,这里是指可变的、不固定的,它能动态地分配时间片,只有当某路信道需要发送数据时才把时间片分配给它,这样就避免了通信信道资源的浪费。

STDM 中各路信号可能并不是以固定的顺序同时出现,所以当数据到达接收端时,接收端不知道应该将哪一个时间片的数据发送到哪一路信道上去。因此,STDM 要求把源端地址、目的端地址等作为附加信息随同数据一起发送,以便接收端能按地址分送数据。STDM 只适用于真正的数字数据传输(如计算机的输出),不适用于经过转换的模拟数据(如 PCM 编码的话音信号)传输。局域网(基带网络)中经常采用这种技术。

(3) 波分多路复用技术

波分多路复用技术(Wave-length Division Multiplexing,WDM)的原理与频分多路复用技术类似,但它主要用于光纤通信。只是光信号是用波长而不用频率来表示所使用的光载波,因此它被称为波分多路复用。WDM 和 FDM,不同之处在于光波频率很高,WDM 是利用不同波长的光,通过共享光纤实现远距离传输多路信号。该技术利用光学系统中的衍射光栅来实现多路不同频率光波信号的合成与分解。

现在可以在一根光纤上复用 80 路或更多路数的光信号,这就是密集波分多路复用(Dense WDM,DWDM)。

3. 数据交换技术

如果不论距离的远近,也不论双方之间数据传输数量的多少,直接在源端和目的端使用物理线路进行通信,显然是不合适的,因为任意两个站点直接专线连接费用太昂贵。相应的解决方法就是设置交换局,采用交换技术。所谓交换技术就是采用交换机或节点机等交换系统,通过路由选择技术在欲进行通信的双方之间建立物理的或逻辑的连接形成一条通路,实现通信双方的信息传输和交换的一种技术。

常用的数据交换方式有两大类:电路交换方式(Circuit Switching)和存储转发交换方式(Store and Forward Switching)。后一种方式中按照被转接的信息单位不同,又可进一步分为报文交换和报文分组交换。

(1) 电路交换方式(Circuit Switching)

它是指在电路交换网络中,通过网络节点在两个工作站之间建立一条专用的通信电路。例如公用电话交换网(PSTN)。使用该方式进行通信时,两个工作站之间使用实际的物理或逻辑连接,该连接由节点的各段电路组成,每一段电路都为该连接提供一条通道。该方式的通信过程包括以下 3 个阶段。

① 建立电路:在传输任何数据之前,都要先建立端到端(站到站)的线路,即在源节点和目的节点间建立一条由各个中间交换节点分段连接所组成的通信电路。

② 传输数据:当通信电路建立以后,就可通过这条专用电路从站点 A 将数据传送到站点 B。当然传输的数据可以是数字数据,也可以是模拟数据。

③ 拆除电路:通信结束后,应由一方立即拆除电路,供其他用户使用。拆除线路信号必须传送到电路所经过的各个节点,以便重新分配资源。

图 2-18 显示的就是从节点 A 到节点 B 所使用的专线 1-5-6-4 进行信息传递的过程。当然从 A 到 B 还有其他专线如 1-2-3-4、1-5-3-4 等,某一个时刻只建立一条专线进行通信即可。

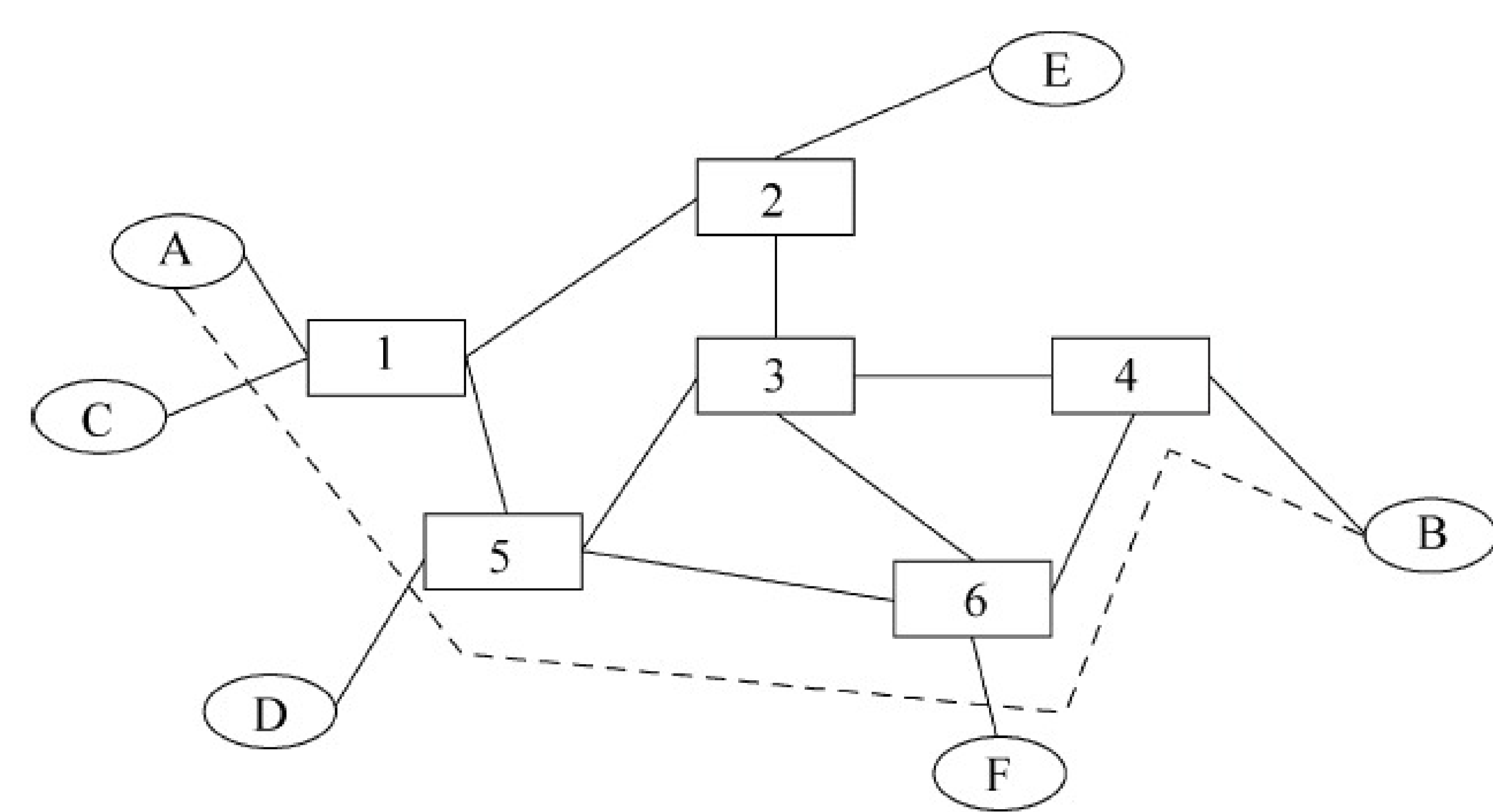


图 2-18 电路交换的过程

电路交换方式中,在传输数据之前建立连接,有延迟;在电路建立后就专用该电路,即使没有数据传输也要占用该电路,利用率较低;一旦建立了连接,网络对于用户就是透明的,用户可以以固定的速率传输数据,此时只有传输延迟。电路交换方式能较好地满足实时性传输,但如果通信量不均匀,就容易引起阻塞。

(2) 报文交换方式(Message Switching)

报文交换属于存储转发交换,其主要原理是把待传送的信息先存储起来,等到信道空闲时再发出去。只要有足够长的存储时间,就能够把信道忙碌和空闲的状态均匀化,有效地压缩了必需的信道容量和转接设备容量,而且利用它的中间存储可以平滑通信和充分利用信道。

报文交换的工作过程如下:发信端将发往收信端的信息分割成一份份的报文正文,再连同收信地址等辅助信息形成一份份的报文。首先发往本地的交换中心(或交换局),并将其存储在交换中心(由于报文一般较长,往往将它存入联机的大容量存储器或脱机的大容量存储器中),当发现去目的地的线路空闲时,再将一份份报文转发到下一个交换中心,依次存储转发直至转到目的地。由于到达目的地的顺序可能发生了变化,所以收信交换中心将收到的各份报文按原来的顺序进行装配,再根据地址信息将完整的信息交付给目的地收信的计算机或终端设备。图 2-19 显示了报文从 A 节点经过中间节点的存储转发,到达 B 节点的传输过程。

报文交换方式以报文为单位发送信息。每个报文由四部分组成:报头(Header)、报文、正文(Message)和报尾(Trailer)。报头由发信站地址、收信站地址及其他辅助信息组成。报尾有时也可以省去,但此情况下的每个报文必须有统一的固定长度。该方式没有拨号呼叫,由报头控制其到达目的地。

(3) 报文分组交换方式(Packet Switching)

报文分组交换方式是 1964 年提出来的,简称为分组交换或包交换,最早在 ARPANET

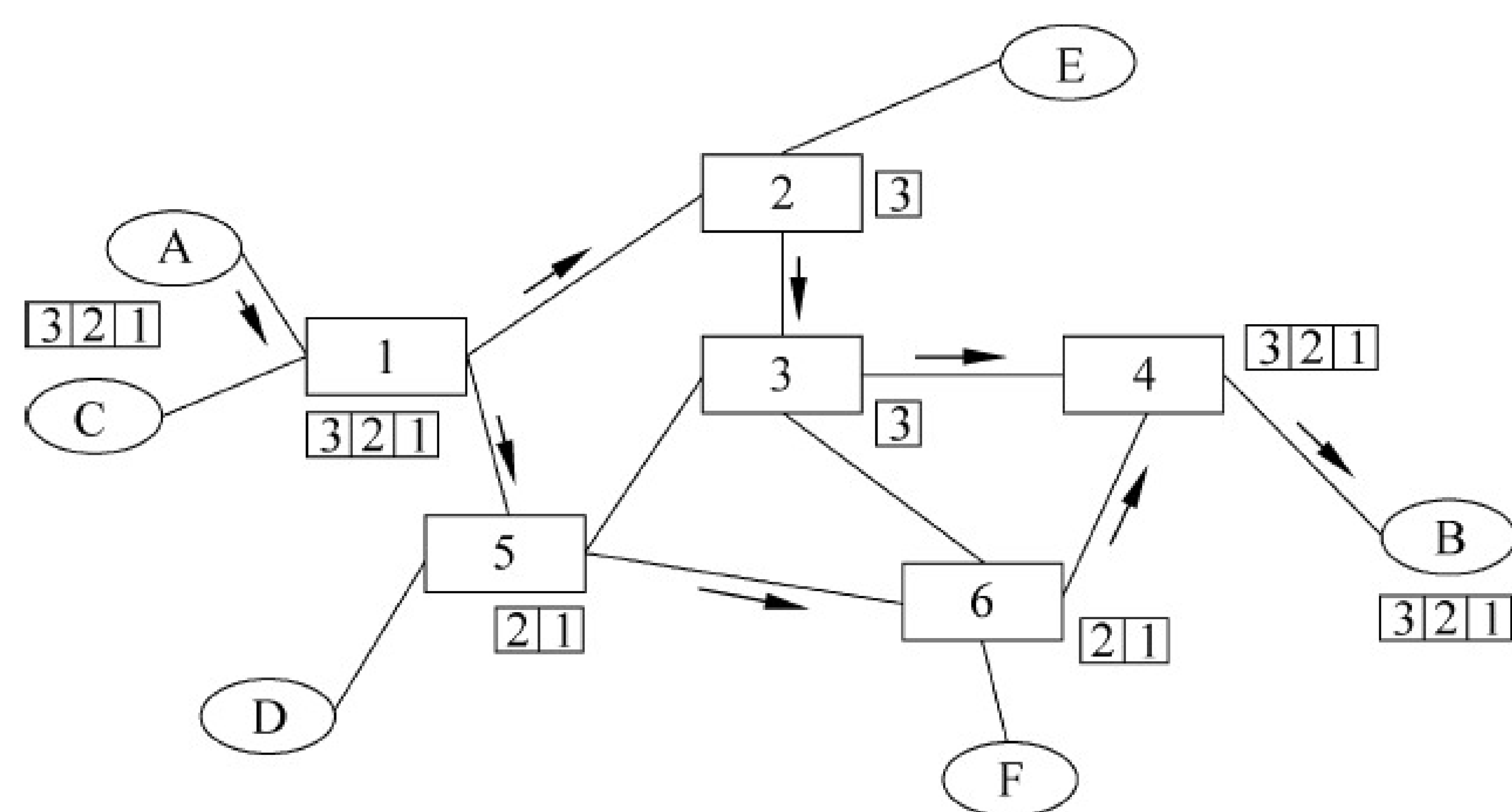


图 2-19 报文交换过程

上得以应用。报文分组交换方式采用了较短的格式化的信息单位,称为报文组(Packet)。在报文分组交换网络中,典型数据单位分组的长度限制在一千比特到数千比特。CCITT(现已改名为 ITU)给报文分组下的定义是:一组包含数据和呼叫控制信号(例如地址)的二进制数,把它作为一个组合整体加以交换,按规定的格式排列这些数据、呼叫信号及可能附加的差错控制信息。由于在发送端已将报文分割成更小的报文分组,使它适合在交换机的主存储器中存储转发,所以与报文交换方式相比,能改善传输的持续时间和传输的延迟时间。

由于采用分组传输以后,发送信息时需要把报文信息拆卸并加入分组报头,接收后还需要去掉分组报头,将分组数据装配成报文信息。所以,用于控制和处理数据传输的软件较复杂,同时对通信设备的要求也较高。报文分组交换中通常采用两种方法来管理分组流:虚电路和数据报。

① 虚电路

在虚电路中,数据在传送之前,发送方和接收方先建立起一条逻辑上的连接(这条逻辑连接并不是一条专用的物理通路),该路径上各个节点都有缓冲设备并服从于这条逻辑线路的安排,也就是按照逻辑连接的方向和接收的次序进行排队和转发,这样每个节点就不需要进行路径判断和选择,就好像收发双方有一条专用通道一样。发送方依次发送的每个数据报经过若干次存储转发后,按顺序到达接收方,双方一旦完成数据交换就拆除这条虚电路。

② 数据报

在数据报中,每个数据报都被独立地处理,同时,每个节点根据一个路由选择算法为每个数据报选择一条路径,使它们的目的地相同。一个节点在发送多个相同地址的数据报时,可以根据当前线路的拥挤情况为各个数据报选择不同的转发节点,所以各个数据报可能是从不同的路径到达目的地的,并且到达的先后顺序也可能不同于分割时的顺序,这要由网络中当时的具体流量等情况来决定。由于在每个数据报中都有相应的分割信息,接收端可以根据这些信息把它们重新组合,以恢复成原来的数据块。

(4) 三种交换方式的优缺点

在电路交换方式中,数据传输可靠、迅速、不丢失且保持原来的序列,但是线路空闲时

的信道容量被浪费。当数据传输不长时,线路的建立和拆除反而得不偿失。它比较适合于系统间要求高质量的大量数据传输的情况。

在报文交换方式中,线路效率较高,不需要同时使用发送器和接收器来传输数据,网络可以在接收器可用之前暂时存储报文,它能把一个报文发送到多个目的地,能够建立报文的优先权,可以进行速度和代码的转换并截获发往未运行的终端的报文。但是,它不能满足实时或交互式的通信要求,不能用于声音连接,也不适合交互式终端到计算机的连接。由于传输延迟大,需要网络节点有大容量的存储设备。

在虚电路分组交换方式中,它能用于两端之间的长时间数据交换,提供了更可靠的通信功能,保证每个分组正确到达且保持原来的顺序。缺点就是当一个节点或某条链路出故障而彻底失效时,所有经过故障点的虚电路将立即被破坏。

在数据报分组交换方式中,没有了呼叫建立阶段,传输少数几个分组的速率比虚电路方式更加简便灵活,还可以绕过故障区而到达目的地。但是它不能保证分组的按序到达,数据的丢失也不会立即知晓。

(5) 其他几种高速交换方式

随着通信和网络应用的发展,传统的交换技术已经不能满足需求。例如,交互式的会话通信要求很高实时性,延时要小;高清晰度电视(HDTV)图像及高速数据的传送要求高速宽带的通信网。现在比较新的高速交换技术主要有:数字语音插空技术、帧中继技术、信元交换技术等。

① 数字语音插空方式

利用数字语音插空方式(Digital Speech Interpolation,DSI)能提高线路交换的传输能力。传统的电路交换技术在接通通路后,该通路被一对用户完全占用。但是在传输语音信号时,通路并不始终处于忙碌的状态,有很多空闲的状态。DSI 技术仅当传输语音信号时,才向通话用户分配通道,其余时刻可把通道分配给数据通信。

② 帧中继方式

帧中继方式(Frame Relay,FR)信息以帧的形式有效地进行传送,使用逻辑连接;完成了信道的动态复用,带宽利用率高,可以实现点到多点的连接;简化了 X.25 的第三层功能,链路层只保留核心子集部分(省去帧编号、流量控制、应答、监视等机制);最大帧长为 1600Byte/frame,适用于网间传输的数据单元,协议开销减少;可占用未预定、未使用的带宽,提高了整个网络资源的利用率,满足用户发送大量数据和突发性业务量的要求。

③ 异步传输模式

异步传输模式(Asynchronous Transfer Mode,ATM)采用信元进行交换。信元由 53 个字符组成,前 5 个字符为信头,完成寻址的功能,后 48 个字符为信息域。它采用统计时分复用技术,可将一个物理通道划分成不同业务特性的多条虚电路提供给用户,实现网络资源的按需分配;具有时延小、实时性好的特点;可提供多种业务、多种用户接口;可实现任意速率的接入,用户改变速率方便灵活;它简化了交换过程,去除了不必要的数据校验,信元格式固定;采用了一些有效的业务流量控制机制,对网上用户数据进行实时监控,把网络拥塞发生的可能性降到最小。

2.2.3　差错控制

在通信过程中，受干扰、设备故障等因素的影响，经常存在被传送的信号失真的现象。差错就是接收方接收的数据与发送方所发送的数据不一致的现象。为了提高传输的准确性，通常要采用专门的校错方法。这些方法的目的在于发现产生的错误，并给出错误出现的位置或校正错误。差错控制就是采用可靠、有效的编码，以减少或消除计算机通信中传输的差错，提高传输质量。

1. 差错控制方法

为了提高传输质量，一是可以改善通信系统的物理性能，使误码率降低到满足要求的程度，但这要受经济上和技术上的限制，难以得到理想的结果。二是采用差错控制方法，它是利用编码的方式将传输中产生的错码检测出来，并加以纠正。在数据通信系统中，差错控制包括差错检测和差错纠正两部分，具体的方法主要有以下几种。

(1) 自动请求重发请求方式(Automatic Repeat Request，ARQ)

在该方式中，接收端只进行差错检测，一旦检测出所接收信息中有错，便自动要求发送端重发，直至收到正确的码字(合法编码)为止。ARQ 方式的系统组成如图 2-20 所示。

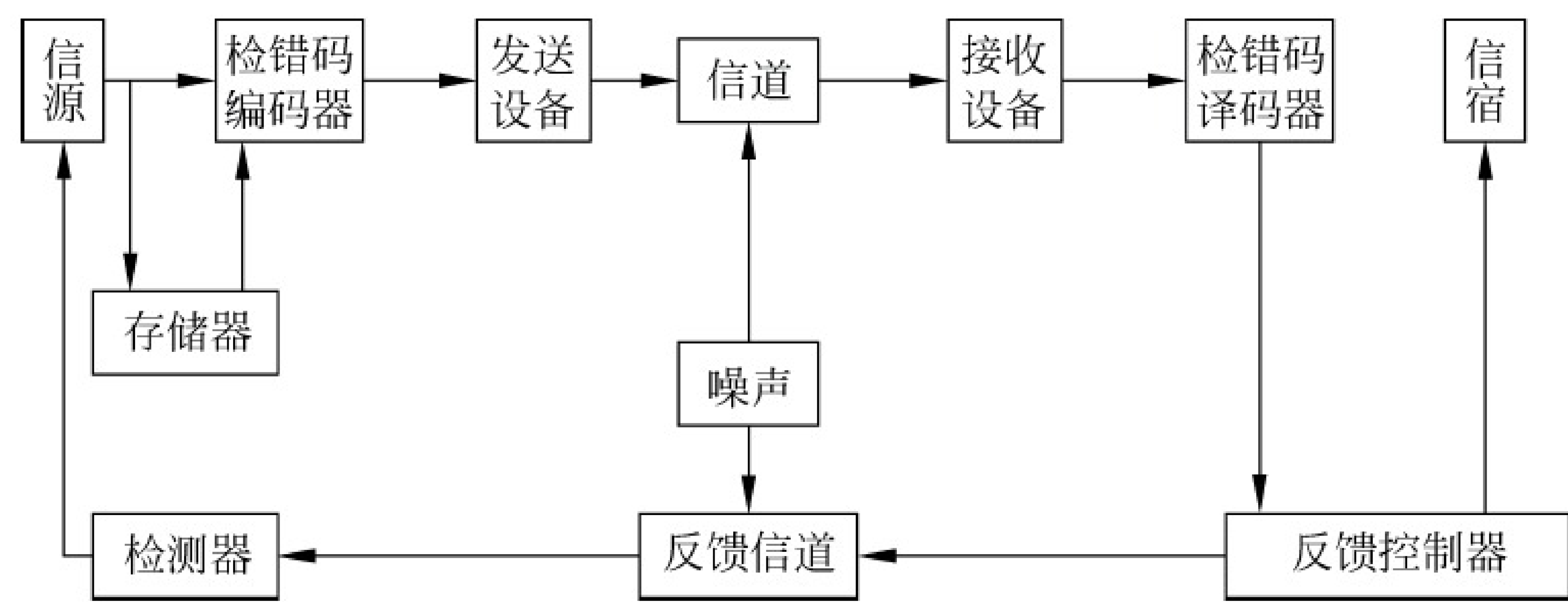


图 2-20　ARQ 纠错系统

具体的控制过程是：信源发送的消息序列，一方面经检错码编码器由发送设备送入信道；另一方面进入存储器以备重发。接收端由检错码译码器对收到的消息序列进行译码，并检测有无错误。若无错，则送出无错信号，经反馈信道送至发送端，通知信源发送下一组消息。同时，通知信宿接收该消息序列。若有错，则通过反馈控制器，使信宿不接收该消息序列，同时通过反馈信道通知发送方重发该消息序列，此时发送端打开存储器，将出错的消息序列再重发一次。

应用 ARQ 方法时必须有反馈信道，而反馈重发的次数与信道受干扰的情况有关，所以如果信道受干扰频繁，则系统经常处于重发状态，导致传送消息的连贯性差。因为接收端只检查有无错误，所以差错检测码和译码设备都比较简单。

(2) 前向纠错法

前向纠错法(Forward Error Correction，FEC)不需要反馈信道传送请求重发消息，但必须用纠错码。接收端收到消息码之后，纠错译码器不仅能发现差错而且能自动纠正差

错，然后将正确的消息送给接收器。但是所用的译码设备比较复杂，而且纠错码与信道噪声干扰情况有关。

(3) 混合纠错法

混合纠错法是将自动请求重发方法和前向纠错方法相互结合。混合纠错法是由发送端同时发出具有检错和纠错能力的编码，接收端收到编码后检查差错情况，如差错可纠正，则自动纠正；如差错很多，超出了纠错能力，则产生的反馈信息经反馈信道送回发送端要求重发。

(4) 反馈检测方法

在该方法中，接收端将收到的每组(或帧)信息码复制后再原封不动地发回发送端，在发送端与刚发的信息码相比较。如果不一致，说明有差错，发送端再重发；如果一致，说明无错，发送端通知接收端将复制的信息接收。这种方法的检错原理和实现很简单，但需要双向信道，而且每组(或帧)信息码至少要在信道中传输两次，效率较低。

前向纠错法和混合纠错法在理论上具有优越性，但由于对应的编码/译码相当复杂，编码效率很低，因而很少被采用。目前绝大多数通信系统所采用的差错控制方式都是自动请求重发(ARQ)方式。

2. 差错控制编码

差错控制主要的任务就是设计具有检错和纠错能力的检错码。实际传输数据位数 T 由两部分组成，K 位信息数据加上 R 位冗余码；用公式 $T=K+R$ 表示。附加 R 位冗余码的作用就是来检验传输数据是否出错，公式中的“+”号表示后续，即数据比特后跟冗余比特。选择 R 位冗余码的常用方法有奇偶校验码、正反码、循环冗余码、海明码等。

(1) 奇偶校验码

奇偶校验码是一种无纠错能力的检错码，其编码规则是先将数据代码分组，在各组数据后面附加一位校验位，使该数据连同校验位在内的码元中“1”的个数为偶数，即为偶校验；为奇数则为奇校验。奇偶校验码纠错能力不强，它只能检测出码元中的任意奇数个错误。

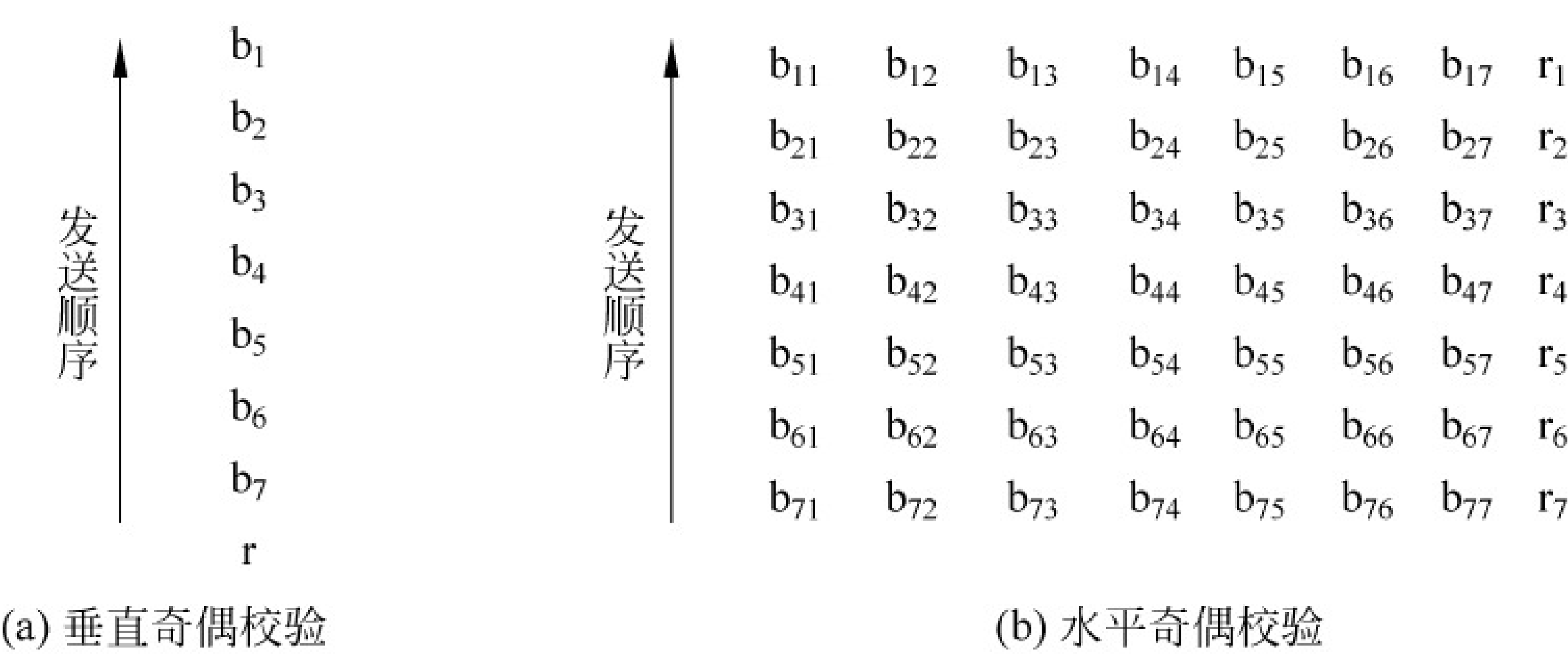
在数据传输时，按奇偶校验码的使用方法，可分为垂直奇偶校验、水平奇偶校验和水平垂直奇偶校验。

① 垂直奇偶校验

发送 $K=7$ 位数据的同时，在加法器中求 K 位数据的和，7 位数据发送完后，一位校验码附加在 K 位数据之后一并发出，接收方将 $7+1$ 位传输代码求和后，与最后一位校验码比较，相同则认为没有出错。

② 水平奇偶校验

发送 $K=7$ 位数据时，发送缓冲区中保留发送副本，发送 7 组数据后，对 7 组数据的每一行求和得出一个水平奇偶校验码。接收方按相同方法求水平校验和，某一行校验正确则表明该行传输没有出错。垂直奇偶校验与水平奇偶校验过程如图 2-21所示。



(a) 垂直奇偶校验　　　　(b) 水平奇偶校验

图 2-21　垂直奇偶校验与水平奇偶校验过程

③ 水平垂直奇偶校验

单独使用垂直奇偶校验或水平奇偶校验，差错漏检率都是 50%。但将这两种方法结合使用，不仅可以提高准确度，有时还可以确定出错比特的位置，从而纠正该错误。水平垂直奇偶校验过程如图 2-22 所示。

发送顺序（↑）

b_{11}	b_{12}	b_{13}	b_{14}	b_{15}	b_{16}	b_{17}	r_{18}
b_{21}	b_{22}	b_{23}	b_{24}	b_{25}	b_{26}	b_{27}	r_{28}
b_{31}	b_{32}	b_{33}	b_{34}	b_{35}	b_{36}	b_{37}	r_{38}
b_{41}	b_{42}	b_{43}	b_{44}	b_{45}	b_{46}	b_{47}	r_{48}
b_{51}	b_{52}	b_{53}	b_{54}	b_{55}	b_{56}	b_{57}	r_{58}
b_{61}	b_{62}	b_{63}	b_{64}	b_{65}	b_{66}	b_{67}	r_{68}
b_{71}	b_{72}	b_{73}	b_{74}	b_{75}	b_{76}	b_{77}	r_{78}
r_{81}	r_{82}	r_{83}	r_{84}	r_{85}	r_{86}	r_{87}	r_{88}

图 2-22　水平垂直奇偶校验过程

(2) 循环冗余码

在实际应用中，如果数据帧大小为超过 10 个比特，用奇偶校验法即可满足要求。对较长的数据帧则使用循环冗余码(Cyclic Redundancy Code，CRC)校验方法。该方法附加位数少，而且检错能力强，其数字逻辑电路也易于实现，是现代网络通信中进行数据帧校验的主要方法。

CRC 方法是一种利用多项式除法进行冗余码生成、接收方检验传输是否出错的有效方法，具体叙述如下。

由公式 $T=K+R$ 可知，在 K 位数据比特后附加上 R 位冗余码组成 T 位传输数据。CRC 首先用相应的多项式表示 K 位数据和 R 位冗余码，由此组成的传输多项式表示 T 位传输代码。

如设 K 位数据位：1011001，那么对应的 $K-1$ 次信息多项式 $K(X)=X^6+X^4+X^3+1$。

R 位冗余码对应一个 $R-1$ 次的冗余多项式 $R(X)$，如果由给出的 $K(X)$能够确定 $R(X)$，那么就可以从多项式 $R(X)$的系数得到相应的 R 位冗余码，也就确定了 T 位传输数据了。

CRC 方法的关键在于引入一个通信双发预先约定的 R 次的生成多项式 $G(X)$，然后用 $X^rK(X)$去模 2 除以 $G(X)$，得到的余式就是 $R(X)$。

例：传输信息系列为 11000110101100，生成多项式 $G(X)=X^4+X^3+1$，求 CRC 码的校验系列码。

解：

将信息写成多项式的形式：

$K(X)=X^{13}+X^{12}+X^8+X^7+X^5+X^3+X^2$

$X^4K(X)$，即将信息位左移 4 位数得：

$M(X)*X^4=X^{17}+X^{16}+X^{12}+X^{11}+X^9+X^7+X^6$

将左移后的多项式 $M(X)*X^4$ 除去生成多项式 $G(X)$，得到余数 $R(X)$：

$R(X)=(M(X)*X^4)\bmod(G(X))=1011$

得到编码多项式 $T(X)$：

$T(X)=M(X)*X^4+R(X)=110001101011001011$

即 CRC 的校验系列码为 110001101011001011。

(3) 海明码(一位纠错码)

海明码是一种可以纠正一位差错的编码。它是利用在信息位为 K 位，增加 R 位冗余位，构成一个 $T=K+R$ 位的码字，然后用 R 个监督关系式产生的 R 个校正因子来区分无错和在码字中的 N 个不同位置的一位错。它必须满足以下关系式：$2^R\geqslant N+1$ 或 $2^R\geqslant K+R+1$。海明码主要用于电话传输编码、串口编码等，传输的距离不能太远。

例如：如果对信息位 10110111001 进行海明编码，由 $2^R\geqslant K+R+1$ 得到 $R=4$，所以需要冗余位是 4 位。$T=K+R=15$，所以海明码为 15 位。如表 2-1 所示，信息位加上冗余位为 15 位的二进制序列。最后一行显示了冗余位与信息位的相互位置，当冗余位 $P1=0$、$P2=0$、$P3=0$、$P4=0$ 时，海明编码信息为：001001100111001。

表 2-1　海明编码

位	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	*		*		*		*		*		*		*		*
		*	*			*	*			*				*	*
				*	*	*	*				*	*	*	*	*
								*	*	*	*	*	*	*	*
冗余位	*P1*	*P2*	1	*P3*	0	1	1	*P4*	0	1	1	1	0	0	1

海明编码的纠错方法：将表 2-1 中的每行进行异或运算得到监督因子，第一行为 S_1，第二行为 S_2，依此类推。将得到的监督因子按 $S_4S_3S_2S_1$ 的顺序写出，如果为 0 表示无错，如果不是 0，出错位对应该因子式的值。

知识拓展——数据传输设备

1. 数据传输模型

数据的传输主要包含以下 5 个部分：

(1) 数据源(Data Source)；

（2）发送器（Transmitter）；

（3）通信信道（Communication Channel）；

（4）接收器（Receiver）；

（5）数据槽（Data Sink）。

如图 2-23 所示为数据传输的模型。

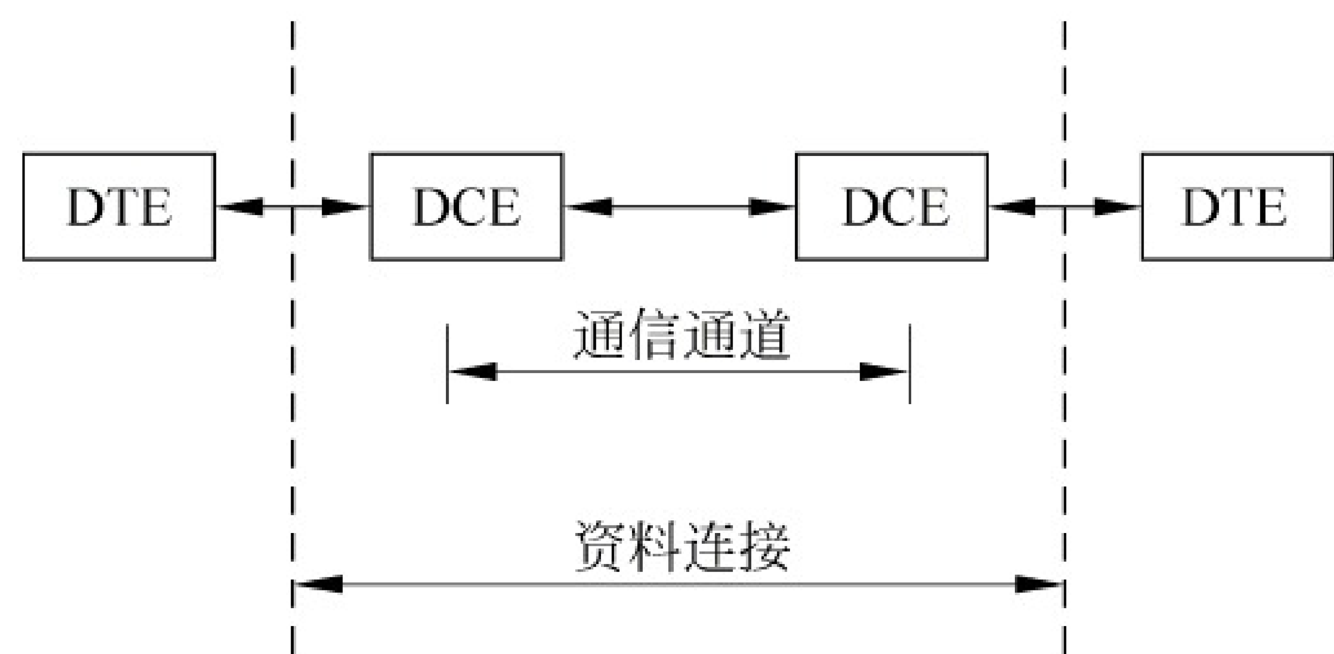


图 2-23　数据传输模型

其中各部分的含义如下。

- DTE——Data Terminal Equipment（数据终端设备）：指的是位于用户网络接口用户端的设备，它能够作为信源、信宿或同时为二者。数据终端设备通过数据通信设备（例如调制解调器）连接到一个数据网络上，并且通常使用数据通信设备产生的时钟信号。数据终端设备包括计算机、协议翻译器以及多路分解器等设备。
- DCE——Data Communication Equipment（数据通信设备）：该设备和其与通信网络的连接构成了网络终端的用户网络接口。它提供了到网络的一条物理连接、转发业务量，并且提供了一个用于同步 DCE 设备和 DTE 设备之间数据传输的时钟信号。调制解调器和接口卡都是 DCE 设备的例子。

2. 传输硬件设备——调制解调器

计算机内的信息是由“0”和“1”组成的数字信号，而在电话线上传递的却只能是模拟电信号。于是，当两台计算机要通过电话线进行数据传输时，就需要一个设备负责数模的转换。这个数模转换器就是调制解调器（Modem）。

计算机在发送数据时，先由调制解调器把数字信号转换为相应的模拟信号，这个过程称为“调制”。经过调制的信号通过电话载波传送到另一台计算机之前，也要经由接收方的调制解调器负责把模拟信号还原为计算机能识别的数字信号，这个过程称为“解调”。正是通过这样一个“调制”与“解调”的数模转换过程，从而实现了两台计算机之间的远程通信。

按照与计算机的连接方式不同，调制解调器可分为内置式调制解调器和外置式调制解调器两类。内置式调制解调器在安装时需要拆开机箱，并且要对中断和 COM 口进行设置，安装较为烦琐。这种调制解调器要占用主板上的扩展槽，但无须额外的电源与电缆，且价格比外置式调制解调器要便宜一些。外置式调制解调器放置于机箱外，通过串行通信口与主机连接。这种调制解调器方便灵巧、易于安装，闪烁的指示灯便于监视调制解调器的工作状况。但外置式调制解调器需要使用额外的电源与电缆。

3. 传输硬件设备——通信适配器(网卡)

计算机与外界局域网的连接是通过主机箱内插入一块网络接口板(或者是在笔记本电脑中插入一块 PCMCIA 卡)。网络接口板又称为通信适配器或网络适配器(Adapter)或网络接口卡 NIC(Network Interface Card),但是现在更多的人愿意使用更为简单的名称"网卡"。

网卡是工作在数据链路层的网络组件,是局域网中连接计算机和传输介质的接口,不仅能实现与局域网传输介质之间的物理连接和电信号匹配,还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。

网卡是网络通信中不可或缺的设备之一,根据接口类型,传输速度,信号模式等可将网卡分为很多类型,相关知识也非常多,感兴趣的读者会随着本课程的深入,逐渐了解。也可以查阅相关资料。

实训 2 分析数据的传输

1. 实训目的

信号可以通过示波器以波形的形式表现出来,不同的信号具有不同的波形单元。通过示波器来观察信号波形,加深对信号编码与调制的理解。

2. 实训设备

示波器一台;

函数信号发生器一台;

元件箱一台;

万用表一个;

晶体管毫伏表一个;

直流稳压电源一个。

3. 实训内容

(1) 按图 2-24 所示方式连接函数信号发生器、示波器,晶体管毫伏表和万用表。

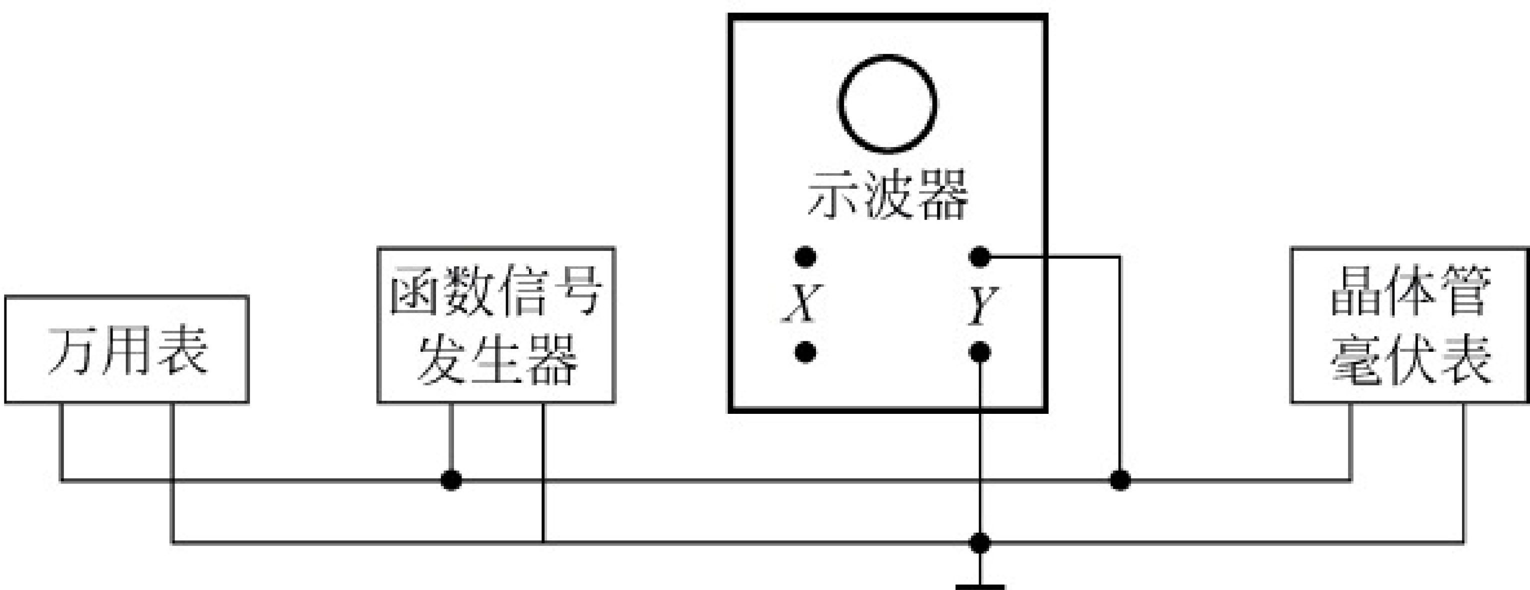


图 2-24 实验连接方式

(2) 使用函数信号发生器产生 400Hz 的正弦信号、方波和三角波,调节示波器使波形稳定,从 Y 轴刻度读出被测信号幅度,并与万用表、晶体管毫伏表读数相比较,如图 2-25 所示。

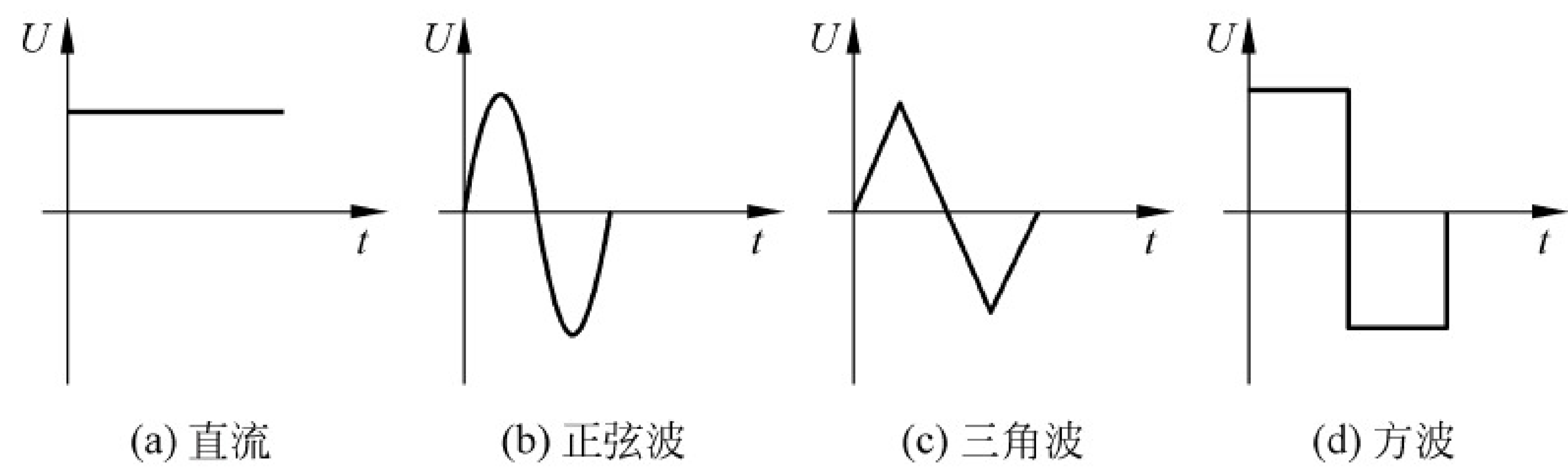


图 2-25 使用示波器观察波形

4. 实训要求

(1) 掌握示波器的使用方法。

(2) 利用波形理解码元和码长等概念。

习 题 2

1. 选择题

(1) 在计算机网络中,DTE 设备兼备( )的作用。

A. 调制解调器　B. 信源　C. 信宿　D. 传输媒体

(2) 在计算机网络中,调制解调器是一种( )设备。

A. ASK　B. DCE　C. DTE　D. PCM

(3) 不归零编码中,单极性不归零编码( )。

A. "0"电平代表 0,正电平代表 1　B. "0"电平代表 1,正电平代表 0

C. 负电平代表 1,正电平代表 0　D. 负电平代表 0,正电平代表 1

(4) 在曼彻斯特编码中( )。

A. 有跳变代表 1,无跳变代表 0

B. 有跳变代表 0,无跳变代表 1

C. 低电平跳到高电平代表 0,高电平跳到低电平代表 1

D. 低电平跳到高电平代表 1,高电平跳到低电平代表 0

(5) 在差分曼彻斯特编码中,在间隔开始时刻( )。

A. 有跳变代表 0,无跳变代表 1　B. 有跳变代表 1,无跳变代表 0

C. 正跳变代表 0,负跳变代表 1　D. 正跳变代表 1,负跳变代表 0

(6) 数据传输速率是指每秒传输构成数据二进制代码的( ) 数。

A. 帧　B. 信元　C. 伏特　D. 比特

(7) ( )是指将数字信号转变成可以在电话线上传输的模拟信号的过程。

A. 解调　B. 采样　C. 调制　D. 压缩

(8) 当 PCM 用于数字化语音系统时,如果将声音分为 64 个量化级,系统的采样速度为 8000 样本/秒,那么数据传输速率应该达到( )。

A. 1200bps　B. 48kbps　C. 2880bps　D. 56kbps

(9) 在脉冲编码调制方法中,首先要进行的步骤是( )。

A. 量化　B. 编码　C. 采样　D. 传输

(10) 在数据交换中,没有延迟的交换技术是(　　)。

A. 电路交换　　B. 报文交换

C. 报文分组交换　　D. 都不是

(11) 计算机网络通信传输的是(　　)。

A. 数字信号　　B. 模拟信号

C. 数字信号或模拟信号　　D. 数字脉冲信号

(12) 误码率描述了数据传输系统正常工作状态下传输的(　　)。

A. 安全性　　B. 效率　　C. 可靠性　　D. 延迟

2. 填空题

(1) 信号是数据的电编码或电磁编码,它可分为________和________两种。

(2) 数据通信可以有________、________和________三种通信方向。

(3) 误码率是指二进制码元在数据传输系统中被传错的________。

(4) 数据传输速率在数值上等于每秒钟传输构成数据编码的二进制________。

(5) 数据通信按传送方式分为________和________两种。

(6) 数据通信系统一般由________、________、________、________几部分组成。

(7) 脉冲编码调制的三个步骤是________、________、________。

(8) ATM 信元长度的字节数是________,信头长度是________。

(9) 常见的差错控制方法有________、________、________、________。

3. 简答题

(1) 什么是波特率?什么是比特率?相应的计算公式是什么?

(2) 传输介质的特性有哪些?常用的传输介质有哪些?各有什么特点?

(3) 什么是调制?什么是解调?分别用 ASK、FSK、PSK 技术调试数据 11010010。

(4) 什么是编码?什么是解码?分别用不归零制、曼彻斯特、差分曼彻斯特技术编码数据 00101101。

(5) 简述并行传输和串行传输的特点,举例说明它们在实际中的应用。

(6) 简述电路交换、报文交换和报文分组交换三种交换的特点。

(7) 传输数据为 11001010101,生成多项式 $G(X)=X^4+X^3+1$,计算 CRC 码的校验码。

模块3 网络体系结构与协议

任务3.1 体系结构与OSI

任务描述：在寄送信件的时候特别注意要写明收件人的地址，一般会具体到街道、门牌号。这样信件才能准确地寄送到目的地。在网络中传输数据，也需要类似于门牌号的地址信息表示目的地，即目的地址。那么网络信息的目的地址是如何表示的？信息从发送端如何到达目的地址指向的接收端呢？首先要从网络的体系结构以及通信协议学起。

1. 网络体系结构

随着计算机网络技术的发展，计算机网络的规模越来越大。网络应用的需求不断增加，网络也因此变得越来越复杂。面对日益复杂化的网络系统，必须采用工程设计中常用的结构化方法，将一个复杂的问题分解成若干个容易处理的子问题，然后逐个加以解决。这种“分而治之”的思想应用在网络系统中就是分层。

分层次是人们对复杂问题处理的基本方法。当遇到一个复杂问题时通常习惯将其分解为若干个小问题，再逐一进行处理。层次化处理方法可以大大降低问题的处理难度，这也是网络研究中采用层次结构的直接动力。

首先来看几个概念。

(1) 协议：计算机网络是由多个互联的节点组成的，节点之间的通信必须遵守一些事先约定好的规则。为网络数据交换而制定的规则、约定与标准被称为网络协议。有了网络协议，网络中各种大小不同、结构不同、操作系统不同、处理能力不同、厂家不同的系统才能连接起来实现互相通信，实现资源共享。从这个意义上讲，协议是网络的本质。

网络协议具有三个要素：语义、语法和时序。

① 语义是用于解释位流每一部分的意义。它规定了需要发出何种控制信息，以及要完成的动作与做出的响应。

② 语法定义了通信双方的数据与控制信息的表现形式，即结构与格式。还规定了数据出现的顺序的意义。

③ 时序是对事件实现顺序的详细说明，即何时进行通信，先发送什么，再发送什么，发送数据的速度等。

(2) 接口：对网络的研究采用了分层次的结构化处理方法，将总体要实现的诸多功能分配在不同的层次中。一个节点内，相邻层之间必然需要信息的交换，比如低层为高层

提供服务等，所以相邻层之间进行信息交换的连接点称为接口。只要接口条件不变，整个系统的工作只与低层的功能有关。只要低层的功能不变，其具体的实现方法和技术可以变化更新，不会影响整个系统运行。

一个功能完备的计算机网络具有相当复杂的结构，同样需要制定一整套复杂的协议集。对于结构复杂的网络，可以采用层次化结构模型。同样，对于复杂的网络协议，最好的组织方式也是层次结构。所以，将网络层次性结构模型与各层协议的集合定义为计算机网络体系结构(Network Architecture)。

网络体系结构研究计算机网络各部分的功能以及各部分之间的交互功能，由一组元素和它们之间的交互方式所定义。网络体系结构对计算机网络应该实现的功能进行了精确的定义，而这些功能是用什么硬件与软件去完成，则是具体实现的问题。网络体系结构是抽象的，而实现是具体的，是指能够运行的一些硬件和软件。

网络体系结构的研究意义：

① 各层之间相互独立。

② 灵活性好。

③ 由于各层独立，因此每层都可以选择最为合适的实现技术。

④ 易于实现与维护。

⑤ 有益于标准化的实现。

2. 开放系统互联参考模型

20 世纪 70 年代末，国际标准化组织(International Standard Organization，ISO)开始为网络通信开发一种概念模型，称为开放系统互联参考模型(Open Systems Interconnection Reference Model，OSI)，它通常被简称为 OSI 参考模型(OSI Reference Model)。1984 年，这个模型成为网络通信的国际标准。

(1) OSI 参考模型的概念

OSI 中的“开放”是指只要遵循 OSI 标准，一个系统就可以与位于世界上任何地方、遵循同一标准的其他任何系统进行通信。

OSI 是分层体系结构的一个实例。每一层是一个模块，用于执行某种主要功能，并具有自己的一套通信指令格式(即协议)。用于相同层的两个功能之间的通信的协议称为对等协议。

OSI 标准的制定采用的是“分而治之”的分层体系结构方法，OSI 参考模型将整个通信功能划分为 7 个层次，分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 3-1 所示。

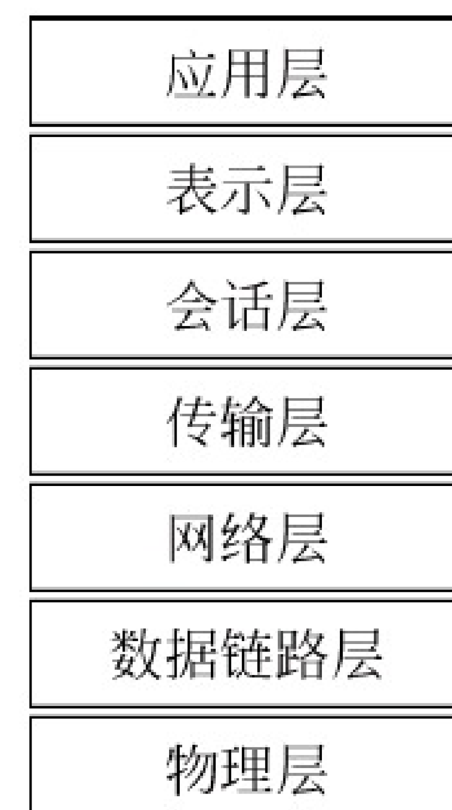


图 3-1 OSI 参考模型

OSI 参考模型划分层次的主要原则是：

① 网络中各节点都具有相同的层次。

② 不同节点的同等层具有相同的功能。

③ 同一节点内相邻层之间通过接口通信。

④ 每一层可以使用下层提供的服务，并向其上层提供服务。

⑤ 不同节点的同等层通过协议来实现对等层的通信。

（2）OSI 参考模型的相关术语

① 数据单元

OSI 参考模型将网络进行了分层，网络中同一节点的相邻层以及不同节点的对等层之间都需要传送数据，所以 OSI 定义了多种类型的数据单元来传送信息。

服务数据单元（Service Data Unit，SDU）是 OSI 参考模型中某层等待传送和处理的数据单元。

协议数据单元（Protocol Data Unit，PDU）指的是在对等层传送的数据单元，它通常是将 SDU 分成若干段，每一段加上报头，作为一个单独协议数据单元 PDU 在水平方向上传送。

如图 3-2 所示，当发送端主机 A 的应用进程数据到达 OSI 参考模型的应用层时，应用层为数据加上本层控制报头后，形成应用层的服务数据单元，然后传输到表示层；表示层收到这个数据单元后加上本层的控制报头，组成表示层的服务数据单元，再传到下一层会话层。依此类推，OSI 参考模型的每层都要形成自己特定的服务数据单元，在节点间的对等层上传输。

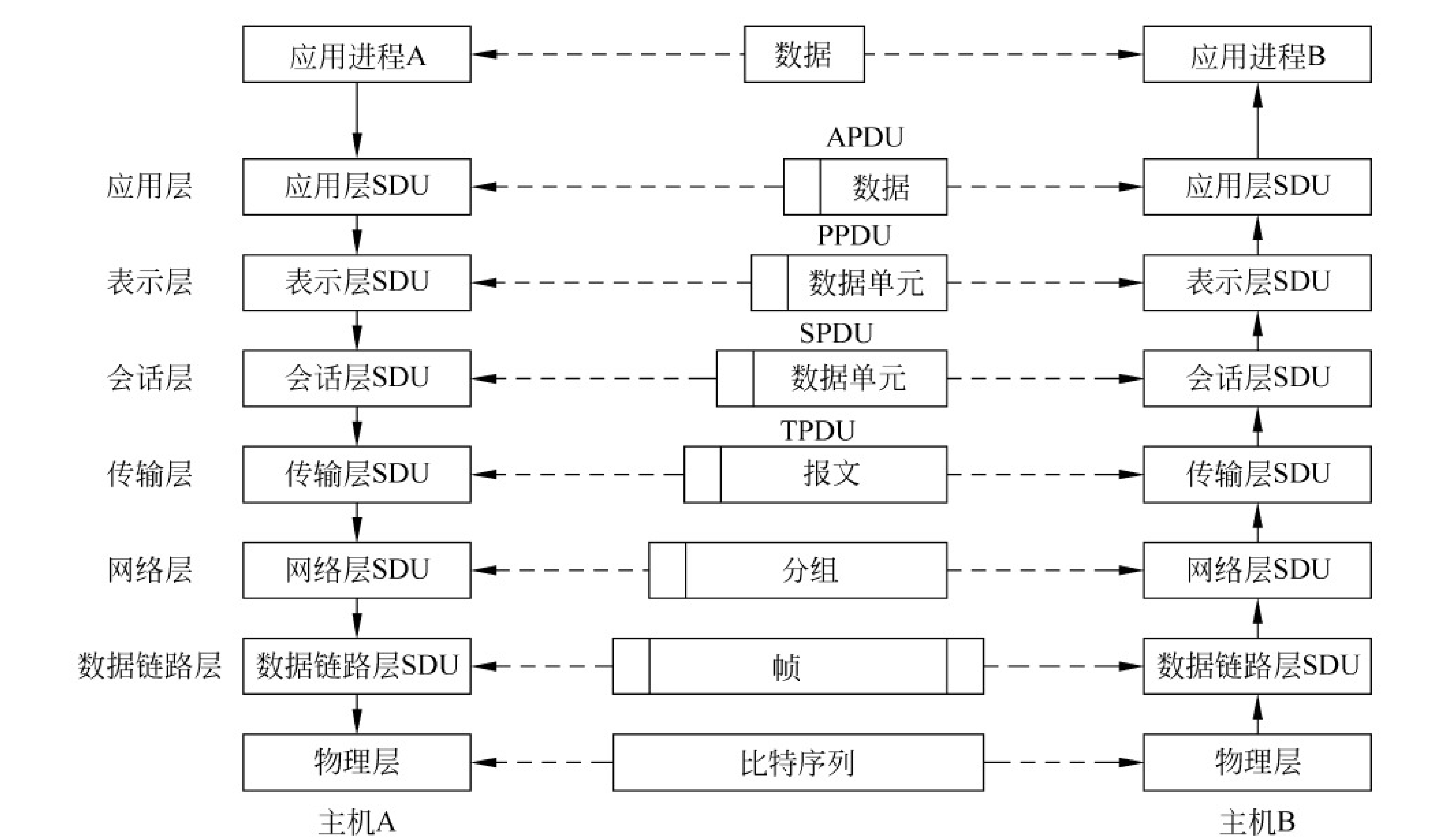


图 3-2　数据单元

通常，在传输层上的服务数据单元被称为报文（Message），网络层上的服务数据单元被称为分组（Packet）。需要注意的是，分组并不是由报文加上网络层的控制报头形成的，由于网络层的数据单元长度有限制，所以传输层的长报文被分成多个较短的数据字段，再加上网络层的控制报头才构成分组。数据链路层的服务数据单元被称为帧（Frame）。在物理层上数据帧将以位流（二进制串）的方式通过传输介质传输。

接口数据单元（Interface Data Unit，IDU）指的是在相邻层接口间传送的数据单元，它由 SDU 和一些控制信息组成。

② 服务访问点

相邻层间的服务是通过其接口界面上的服务访问点(Service Access Point,SAP)进行的,每个 SAP 都有一个唯一的地址。

③ 服务原语

某一层为其上一层提供的服务通常是由一组原语(Primitive)操作来组成的,用户进程通过这些原语操作可以访问该服务。例如,原语 LISTEN 的含义是等待一个进入的连接,原语 CONNECT 的含义是与一个正在等待的对等体建立连接。

服务与协议是截然不同的概念,它们的区别非常重要。如图 3-3 所示,服务是指某一层向它上一层提供的一组原语(操作)。服务定义了该层打算代表其用户执行哪些操作,服务也会涉及两层之间的接口,其中底层是服务提供者,而上层是服务的用户。

协议是一组规则,用来规定同一层上的对等实体之间所交换的消息或这分组的格式和含义。这些实体利用协议来实现它们的服务定义。

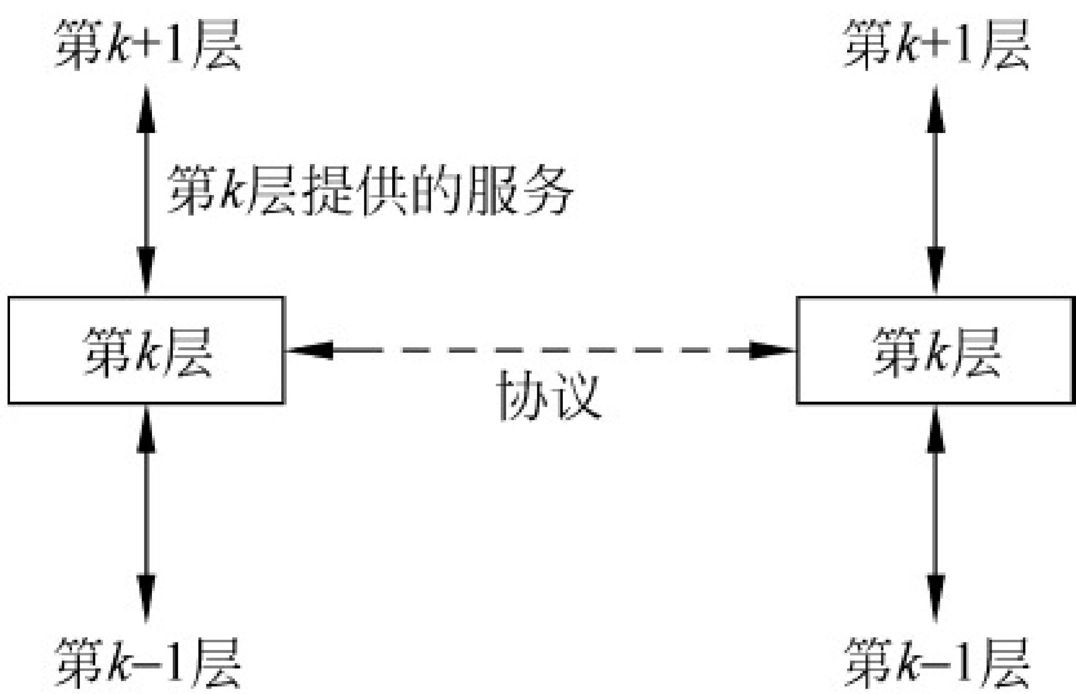


图 3-3 服务与协议的关系

3. OSI 参考模型的工作过程

图 3-4 描述了 OSI 环境中,网络中一个节点(网络上的计算机等设备在实际中被称为节点(Node)),如主机 A 与另一个节点(主机 B)的通信过程。详细说明了数据在同一个节点中的不同层次间传输以及在不同节点的同等层间的传输过程。

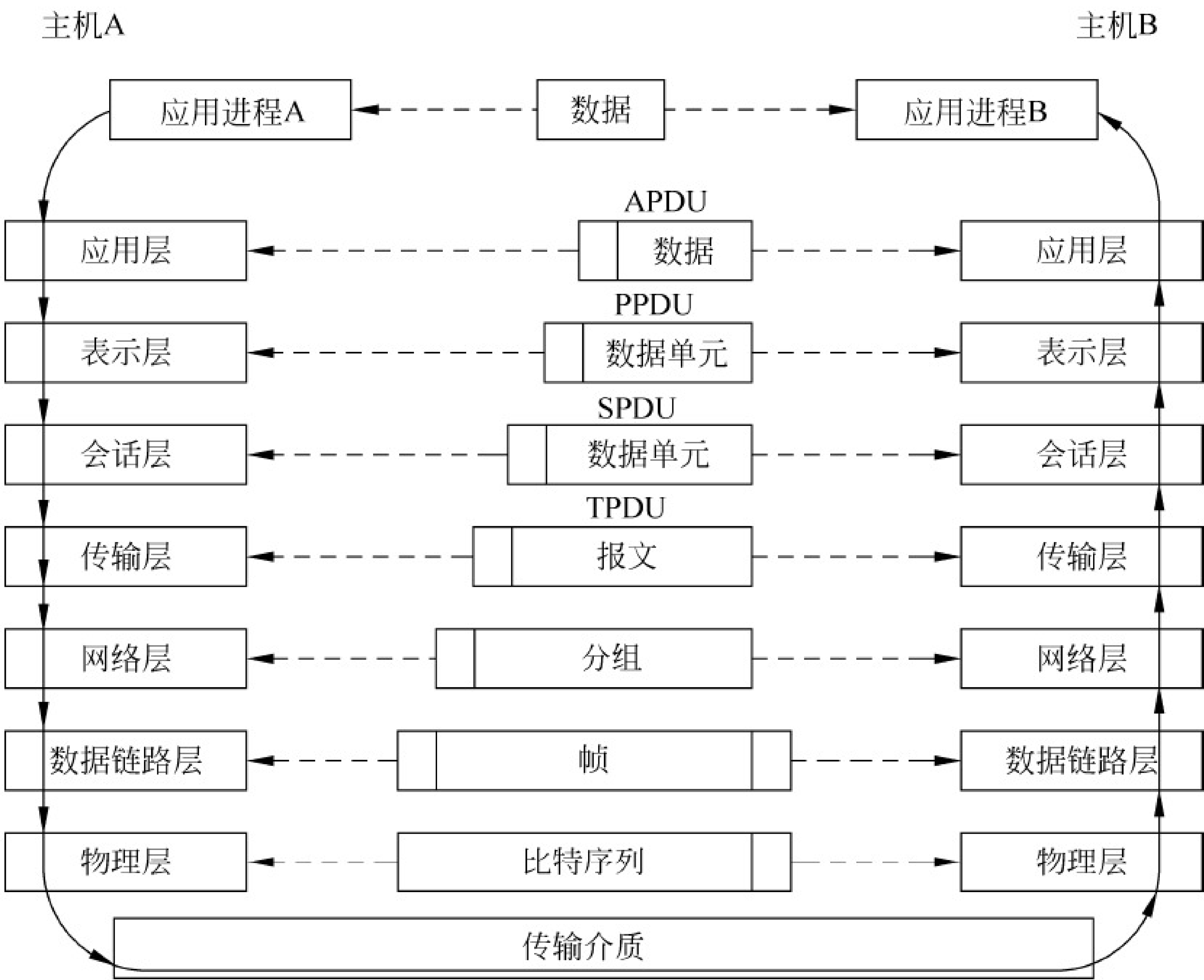


图 3-4 OSI 环境中数据的传输

当数据被网络节点发送时，数据就在 OSI 栈中向下移动，并且每一层都会用自己的标记标识数据，形成自己的数据单元，最终被发送到网络介质中。当数据被某个节点，比如网上的另外一台计算机接收之后，它就在 OSI 栈中向上移动，直到又变成能被那台计算机上的用户访问的数据形式。在表 3-1 中可以看到，OSI 模型中的每一层都负责某个特定的任务，如将用户数据转换为能够在网络上发送的形式、负责建立和维持通信节点之间的连接、负责数据寻址以及决定数据的来源（在哪个节点上发送）和数据的目的地等。

任务 3.2 OSI 各层功能介绍

OSI 参考模型的层次是相互独立的，每一层都有各自独立的功能。下面介绍 OSI 参考模型中各层的主要功能。

1. 物理层

物理层是 OSI 参考模型的底层，向下直接与物理传输介质相连接。该层负责实现两个物理设备之间二进制位流的透明传输，即对数据链路层屏蔽物理传输介质的特性。

物理层传输数据的单位是二进制位。需要注意的是，物理层并不是指连接计算机的具体的物理设备或具体的传输媒体。物理层的作用是，尽可能地屏蔽种类繁多的物理设备或传输媒体之间的差异，对上一层即数据链路层提供统一的服务。所以物理层主要关心的是在连接各种计算机的传输媒体上传输数据的位流。为了达到这个目的，物理层在设计时涉及的主要问题有：

（1）用多大的电压代表二进制“1”或“0”，以及当发送端发出“1”时，在接收端如何识别出这是二进制位“1”而不是二进制位“0”。

（2）确定连接电缆材质、引线的数目及定义、电缆接头的几何尺寸、锁紧装置等。

（3）指出一个比特信息占用多长时间。

（4）采用什么样的传输方式。

（5）初始连接如何建立。

（6）当双方结束通信时如何拆除连接。

综上所述，物理层提供为建立、维护和拆除物理链路所需要的机械的、电气的、功能的和规程的特性。

2. 数据链路层

数据链路层传输数据的单位是帧（Frame），数据帧的帧格式中包括的信息有：地址信息部分、控制信息部分、数据部分、校验信息部分。数据链路层的主要作用是通过数据链路层协议（即链路控制规程），在不太可靠的物理链路层上实现可靠的数据传输。

为了完成这一任务，数据链路层必须执行链路管理、帧传输、流量控制、差错控制等功能。数据链路层向网络层提供的基本服务有：

（1）数据链路建立、维护与释放的链路管理工作。

（2）数据链路层服务数据单元帧的传输。

(3) 差错检测与控制。

(4) 数据流量控制。

(5) 帧接收顺序控制。

(6) 在多点连接或多条数据链路连接的情况下,提供数据链路端口标识的识别,支持网络层实体建立网络连接。

总之,数据链路层把一条有可能出差错的实际链路,转变为由网络层向下,看起来好像是一条不出差错的链路。

3. 网络层

网络层传送的数据单位是分组(Packet),即数据包。在计算机网络中进行通信的两个计算机之间可能要经过许多个节点和链路,也可能经过多个路由器连接的通信子网。网络层的任务就是要选择最佳的路径,使发送节点的传输层所传下来的报文能够正确无误地按照目的地址找到目的节点的网络层,并交付给目的节点的传输层。这就是网络层的路由选择功能。

路由选择指的是根据一定的原则和算法在传输通路上选出一条通向目的节点的最佳路径。路由选择是广域网和网际网中非常重要的问题,局域网则比较简单,甚至可以不需要路由选择功能。路由选择的好坏在很大程度上决定了网络的性能,如网络吞吐量(在一个特定的时间内成功发送数据包的数量),平均延迟时间、资源的有效利用率等。一个好的路由选择应有以下特点:

(1) 信息传送所用时间最短。

(2) 使网络负载均衡。

(3) 通信量均匀。

(4) 路由选择算法简单易实现,不至于因拓扑的变化,影响报文正常到达目的节点。

4. 传输层

传输层传送的信息单位是报文(Message)。传输层的基本功能是从会话层接收数据报文,封装后交给网络层。传输层在发送较长的报文时,首先把报文分割成若干个报文分组,然后再交给下一层(即网络层)进行传输。另外,传输层还负责报文错误的确认和恢复,以确保信息的可靠传递。

OSI 参数模型所定义的传输层是中间层,是通信子网(下 3 层)和资源子网(上 3 层)的分界线。传输层屏蔽通信子网的物理差异,完成资源子网中两节点的直接逻辑通信,实现通信子网中端到端的透明传输,使高层用户感觉不到通信子网的存在。另外,传输层还要处理端到端的差错控制和流量控制的问题。

5. 会话层

会话层负责在发送节点和目的节点之间建立通信链接或会话(Session),会话层还负责管理已经在这两个节点之间建立起来的通信会话。

会话层的另外一个功能是,在发送节点向目的节点传送的数据流中加入特殊的检查点。如果节点之间的连接丢失,这些检查点就可以发挥作用。发送节点不需要重现发送所有的数据,只需从最近接收到的检查点处开始的数据发送即可。

6. 表示层

表示层可被认为是 OSI 参考模型中的翻译器，该层从会话层取得数据，然后将其转换为接收节点的应用层能够读取的格式。表示层也负责数据加密和数据压缩。所以，表示层为上层(应用层)提供共同需要的数据或信息语法的表示变换。

7. 应用层

应用层是 OSI 参考模型的最高层，是计算机网络与最终用户的界面，为网络用户之间的通信提供专用的程序。OSI 参考模型的 7 层协议从功能划分来看，下面 6 层主要解决支持网络服务功能所需要的通信和表示问题，应用层则提供完成特定网络功能服务所需要的各种应用协议，比如消息处理、文件传输和数据库查询。应用层还负责同步客户机/服务器之间的应用程序，保证从错误中恢复所需的资源，并提供数据完整性。

表 3-1 总结了 OSI 参考模型各层的主要功能。

表 3-1　OSI 参考模型各层的主要功能

OSI 层	功　　能
应用层	在程序之间传递信息
表示层	处理文本格式化，显示代码转换
会话层	建立、维持、协调通信
传输层	确保数据正确发送
网络层	决定传输路由，处理信息传递
数据链路层	编码、编址、传输信息
物理层	管理硬件连接

任务 3.3　TCP/IP 体系结构

3.3.1　TCP/IP 参考模型的发展

1. TCP/IP 参考模型的起源

OSI 参考模型研究的初衷是希望为网络体系结构与协议的发展提供一种国际标准。但是，不能不看到 Internet 在世界范围内的飞速发展以及 TCP/IP 协议的广泛应用对网络技术发展的影响。虽然 TCP/IP 协议不是 OSI 标准，但它们是目前最流行的商业化的协议，并被公认为当前的工业标准或“事实上的标准”。

在 TCP/IP 协议出现后，出现了 TCP/IP 参考模型。1974 年，Kahn 定义了最早的 TCP/IP 参考模型。1985 年，Leiner 等人对它开展了进一步研究。1988 年，Clark 在参考模型出现后对其设计思想进行了讨论。

2. TCP/IP 协议的特性

Internet 上的 TCP/IP 协议之所以能够迅速发展起来，不仅因为它是美国军方指定使用的协议，更重要的是它恰恰适应了世界范围内的数据通信的需要。TCP/IP 协议具有以下 4 个特点。

(1) 开放的协议标准，可以免费使用，并且独立于特定的计算机硬件与操作系统。

(2) 独立于特定的网络硬件，可以运行在局域网、广域网，更适用于互联网中。

(3) 统一的网络地址分配方案，使得整个 TCP/IP 设备在网中都具有唯一的地址。

(4) 标准化的高层协议，可以提供多种可靠的用户服务。

3.3.2 TCP/IP 参考模型

在如何用分层模型来描述 TCP/IP 参考模型的问题上争论很多，但共同的观点是 TCP/IP 参考模型的层次数比 OSI 参考模型的 7 层要少。图 3-5 给出了 TCP/IP 参考模型与 OSI 参考模型的层次对应关系。

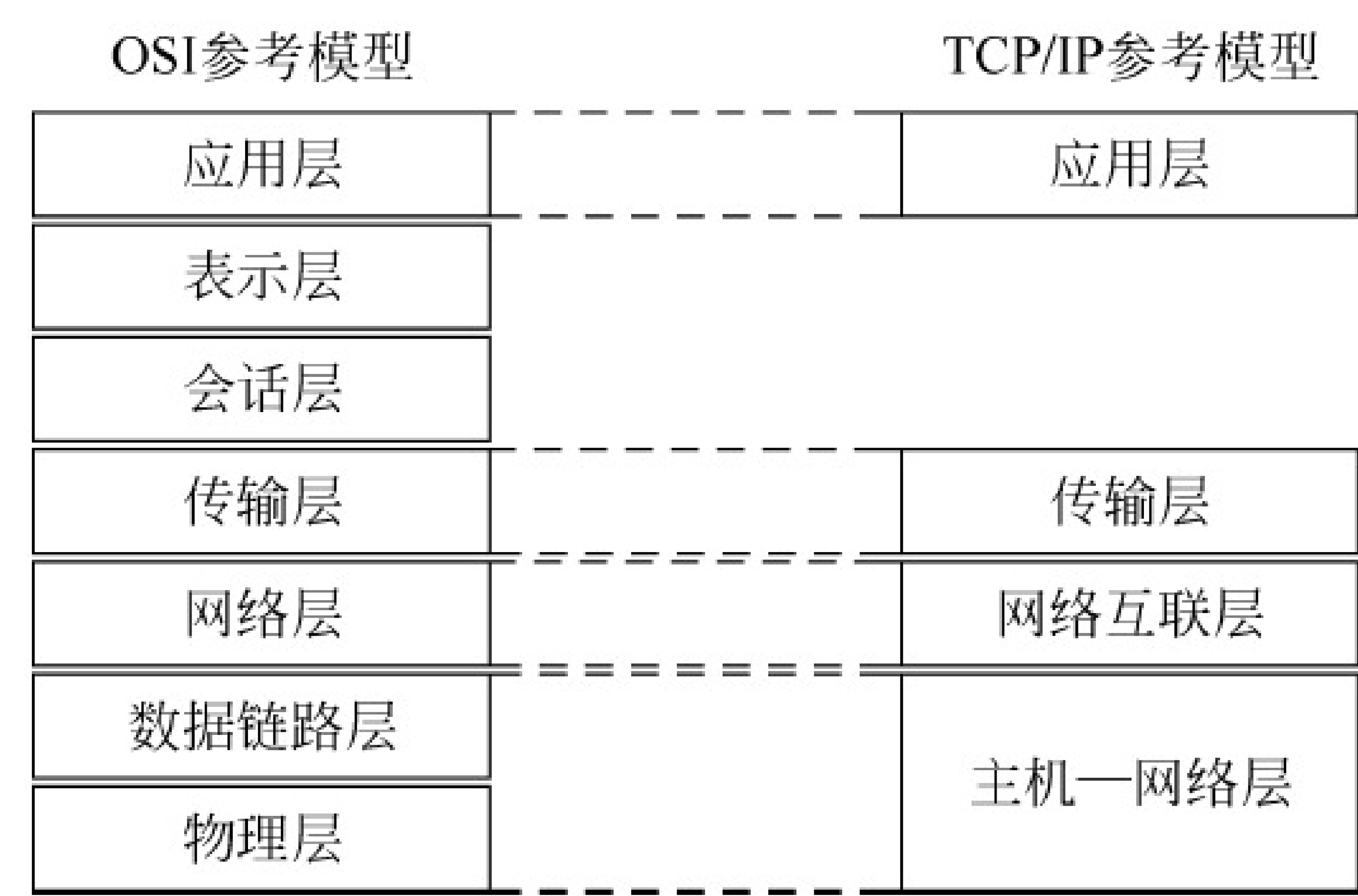


图 3-5 TCP/IP 参考模型与 OSI 参考模型的层次对应关系

TCP/IP 参考模型可以分为 4 个层次：应用层(Application Layer)、传输层(Transport Layer)、网络互联层(Internet Layer)和主机—网络层(Host-to-Network Layer)。

其中，TCP/IP 参考模型的应用层与 OSI 参考模型的应用层相对应；TCP/IP 参考模型的传输层与 OSI 参考模型的传输层相对应；TCP/IP 参考模型的网络互联层与 OSI 参考模型的网络层相对应；TCP/IP 参考模型的主机—网络层与 OSI 参考模型的数据链路层和物理层相对应。在 TCP/IP 参考模型中，对 OSI 参考模型的表示层和会话层没有对应的协议。

1. 主机—网络层

主机—网络层(又称网络接口层)与 OSI 参考模型的数据链路层和物理层相对应，它不是 TCP/IP 协议的一部分，但它是 TCP/IP 赖以存在的与各种通信网之间的接口，所以，TCP/IP 对该层并没有给出具体的规定。

2. 网络互联层

网络互联层的主要功能是使主机可以把分组发往任何网络并使分组独立地传向目标(可能经由不同的网络)。这些分组到达的顺序和发送的顺序可能不同，因此，如果需要按顺序发送及接收时，高层必须对分组排序。这就像一个人邮寄一封信，不管他准备邮寄到哪个国家，他仅需要把信投入邮箱，这封信最终会到达目的地。这封信可能会经过很多的国家，每个国家可能有不同的邮件投递规则，但这对用户是透明的，用户不必知道这些投递规则。网络互联层有 4 个主要的协议：网际协议(Internet Protocol，IP)、互联网控制报文协议(ICMP)、地址解析协议(ARP)和逆向地址解析协议(RARP)。

网际协议的基本功能是：无连接的数据报传送和数据报的路由选择，即 IP 协议提供主机间不可靠的、无连接的数据报传送。互联网控制报文协议提供的服务有：测试目的地的可达性和状态、报文不可达的目的地、数据报的流量控制、路由器路由改变请求等。地址解析协议的任务是查找与给定 IP 地址相对应主机的网络物理地址。逆向地址解析

协议主要解决物理网络地址到 IP 地址的转换。

3. 传输层

TCP/IP 的传输层提供了两个主要的协议,即传输控制协议(TCP)和用户数据报协议(UDP),它的功能是使源主机和目的主机的对等实体之间可以进行会话。

传输控制协议是面向连接的协议。所谓连接,就是两个对等实体为进行数据通信而进行的一种结合。面向连接服务是在数据交换之前,必须先建立连接。当数据交换结束后,则应终止这个连接。面向连接服务具有连接建立、数据传输和连接释放这三个阶段。在传送数据时是按序传送的。

用户数据协议是无连接的服务。在无连接服务的情况下,两个实体之间的通信不需要先建立好一个连接,因此,其下层的有关资源不需要事先进行预订保留。这些资源将在数据传输时动态地进行分配。无连接服务的另一特征就是它不需要通信的两个实体同时处于激活状态。当发送端的实体正在进行发送时,它才必须是活跃的。无连接服务的优点是灵活方便和比较迅速。但无连接服务不能防止报文的丢失、重复或失序。无连接服务特别适合于传送少量零星的报文。

4. 应用层

在 TCP/IP 参数模型体系结构中并没有 OSI 参数模型的会话层和表示层,TCP/IP 参数模型把它都归到应用层。所以,应用层包含所有的高层协议,如虚拟终端协议(TELNET)、文件传输协议(FTP)、简单邮件传送协议(SMTP)和域名服务(DNS)等。

任务 3.4 TCP/IP 协议栈

按照层级结构思想对网络模块化的研究,其结果是形成一组从上到下单向依赖关系的协议栈(Protocol Stack),也叫做协议族。TCP/IP 参考模型与 TCP/IP 协议栈之间的关系如图 3-6 所示。

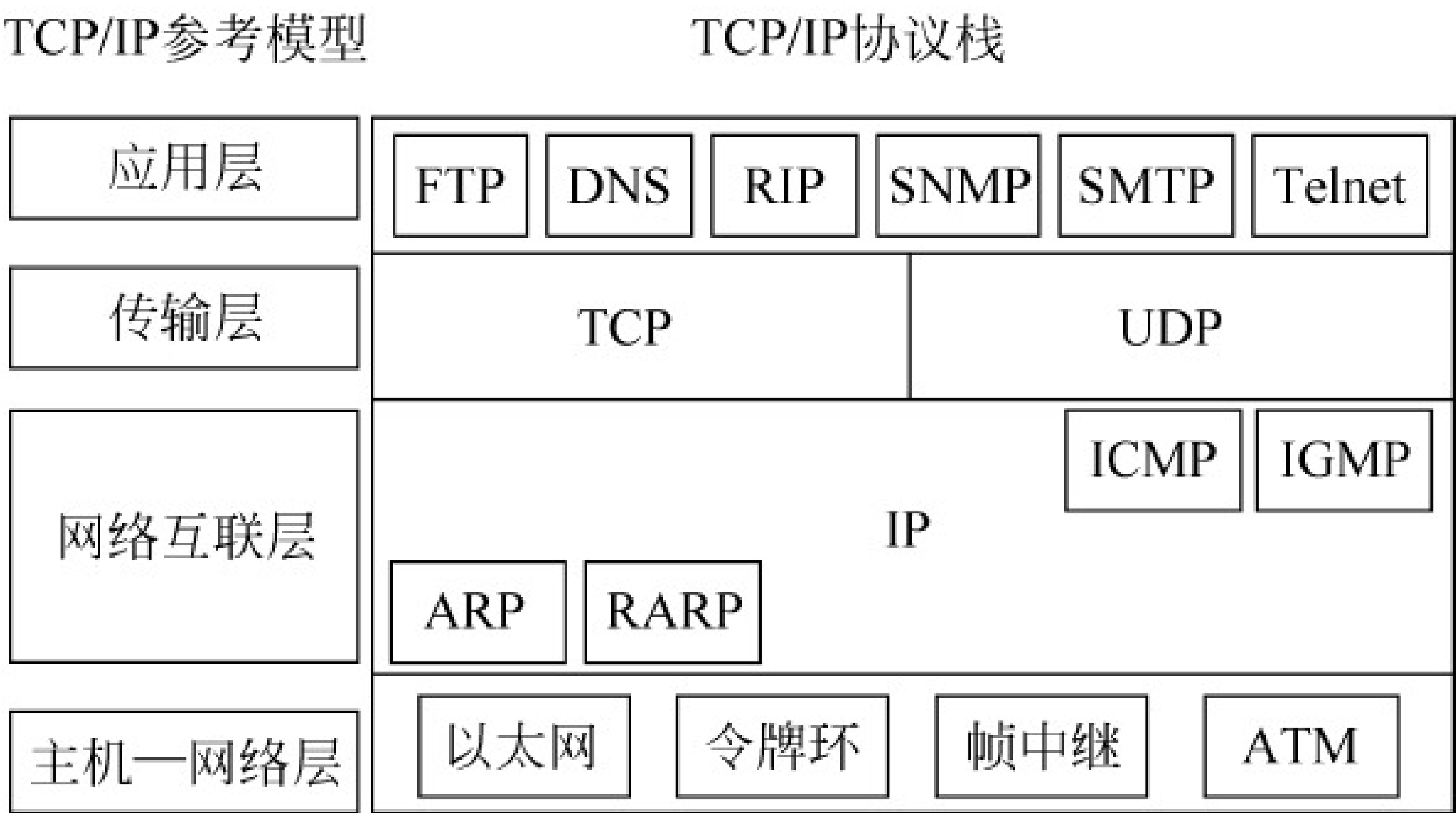


图 3-6 TCP/IP 参考模型与 TCP/IP 协议栈之间的关系

3.4.1 IP 协议

IP 协议即 Internet Protocol,网际协议。规定了如何对数据包进行寻址和路由,并且把数据包从一个网络转发到另一个网络。还规定了计算机在 Internet 上通信所必须遵守

的一些基本规则，以确保路由的正确选择和报文的正确传输。

1. IP 地址含义及获得

在 Internet 中为了定位每一台计算机，需要给每台计算机分配或指定一个确定的“地址”，称为 Internet 的网络地址。即用 Internet 协议语言表示的地址。目前 IP 地址仍然使用 IPv4 协议版本。IPv4 的 IP 地址由 32 位二进制位组成，它逻辑上分成两个部分，一部分标识主机所属的网络（网络标识）；另一部分标识主机本身（主机标识）（如图 3-7 所示）。

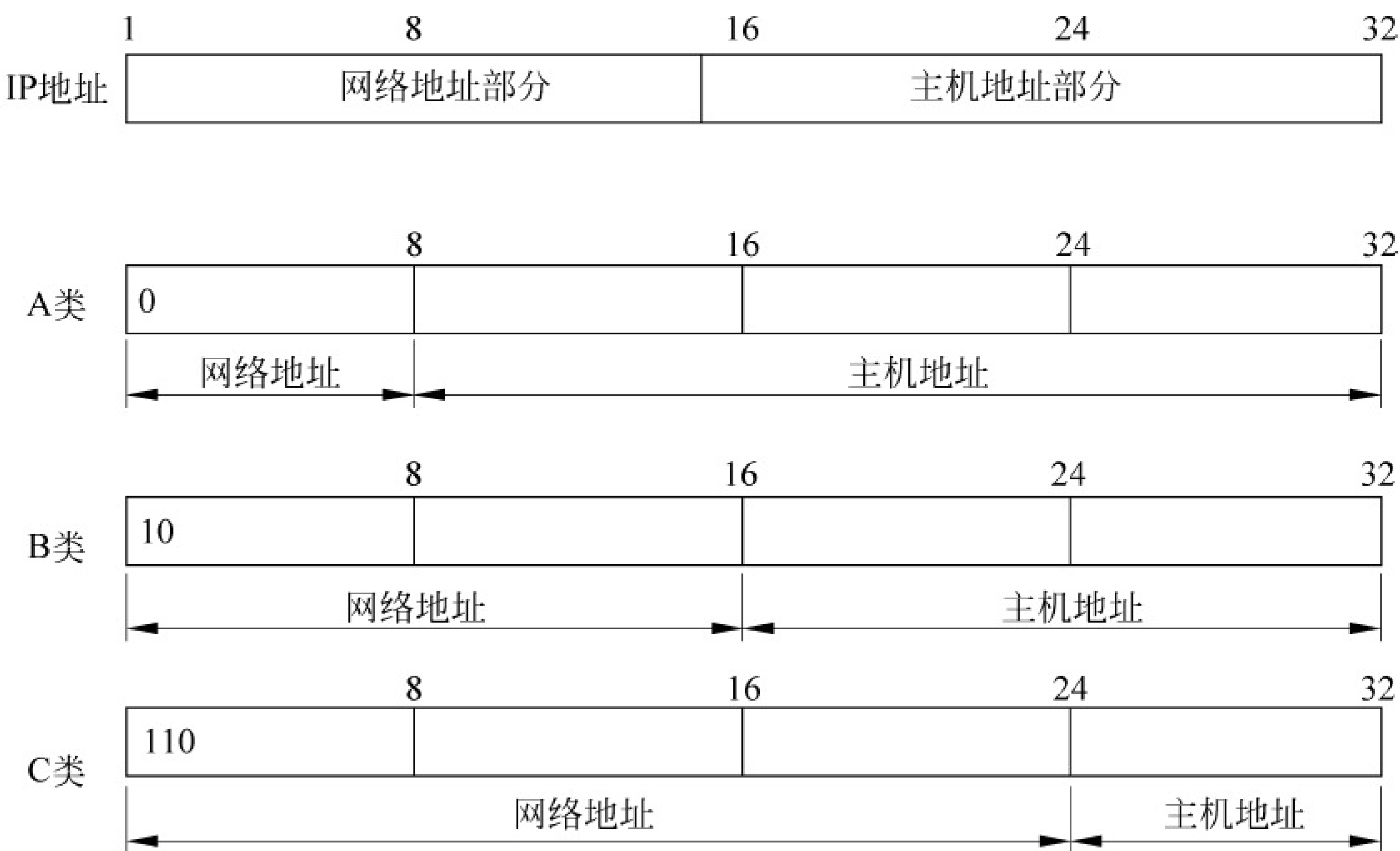


图 3-7　IP 地址

为了方便，IP 地址一般用圆点隔开的 4 个十进制数表示，如某个 IP 地址为：192.168.0.81，其中每个十进制数都是 0～255 间的整数。

常见的 IP 地址分为 A、B、C 三类，与它对应的网络有时被称为 A 类网络、B 类网络、C 类网络。

A 类网络用第一个字节标识网络本身，后面三组数字作为连接于网络上的主机的地址，并且规定第一个字节的第一位必须为 0。A 类 IP 地址一般分配给国家级网络。

B 类网络用第一、第二字节表示网络地址，后面两组数字代表网络上的主机地址，且第一个字节的前两位为 10。B 类 IP 地址一般分配给大型网络，如跨国公司的大型网络。

C 类网络用前三个字节表示网络的地址，最后一组数字作为网络上的主机地址，且第一个字节的前三位为 110。C 类 IP 地址分配给小型网络，如大量的局域网和校园网。

关于 IP 地址的详细介绍参看模块 5 的相关部分。

2. IP 分组格式

网络层传输的数据单元是 IP 数据报（IP 分组），IP 协议对 IP 数据报的报文格式进行了详细的规定。每个 IP 数据报包含一个头部和一个正文部分。而 IP 数据报的头部决定了数据报的正确性及是否能被正确传输。IP 数据报的头部由一个 20 字节的定长部分和一个可选的变长部分构成。图 3-8 显示了 IP 数据报的头部格式。

<table>
<tr><td>IP版本号4</td><td colspan="2">IP分组头
首部长度4</td><td>服务类型8</td><td colspan="2">总长度16</td></tr>
<tr><td colspan="4">标识符</td><td>标志3</td><td>段偏移13</td></tr>
<tr><td colspan="2">生存时间</td><td colspan="2">协议</td><td colspan="2">分组头校验和</td></tr>
<tr><td colspan="6">源站地址(发送IP分组的源主机IP地址)</td></tr>
<tr><td colspan="6">目的站地址(目的主机IP地址)</td></tr>
<tr><td colspan="6">任选参数选项(根据需要可以改变)</td></tr>
<tr><td colspan="6">填充段(可变，通常用0填入，可使IP分组满足4字节长度的整数倍)</td></tr>
</table>

图 3-8　IP 分组格式

IP 版本号：标示协议的版本号，记录了数据报属于哪个版本的协议。目前依然使用 IPv4 协议。

IP 分组头首部长度：表示 IP 分组头的长度(取值的范围是 5～15)。首部最大长度为 60 字节。

服务类型：给出了数据报传送过程中对服务质量的请求，该请求通常由路由器处理。

总长度域：说明该数据包的长度，包括报头和数据部分。IP 分组最大长度为 65 536 字节。

标识符域：使源站唯一的标识一个未分段的 IP 分组，该分组的标识符、源站和目的地址都相同，且协议字段也相同。

标志段：含有控制标志，第一位必须为 0；第二位(不可分段位 DF)：置 1 数据报禁止分段；第三位(还有分组段位)：置 1 表示不是最后的不分组段。

段偏移：表明当前分组段在原始 IP 数据分组报文中数据起点的位置。

生存时间：IP 分组在 Internet 中停留的最长时间 TTL。每过一个路由器减 1。

协议：协议字段指出此数据报携带的传输层数据是何种协议，使目的主机的 IP 层知道将此数据上交给哪个进程。常用的一些协议和相应的协议字段的值为：1(ICMP 协议)、6(TCP 协议)、8(外部网关协议(EGP))、17(用户数据报协议(UDP))等。

分组头校验和：保证了 IP 分组头值的完整性，检验和每过一个路由器都要重新计算。每两个字节为一个单位相加，有进位加 1，直到加完。最后的和值对 1 求补，即得到 16 位的检验和。

IP 数据报选项：字段主要用于网络测试或调试。但是选项的处理是 IP 协议的组成部分，因此所有的标准实现必须将其包括在内。选项包括：记录路由选项、源路由选项、时间戳选项等。

路由和时间戳选项：提供了一种监视或控制互联网路由器路由数据报的方法。记录路由选项允许源站生成一个 IP 地址的空表，并处理过该数据报的每个路由器将其 IP 地址加入表中。当数据报到达目的主机能提取和处理该 IP 地址表。

源路由选项：提供了一种由源站点指定一条通过互联网的路径的方法。分为严格源路由选择：规定数据报要经过指定的地址到达目的主机。表中路径上相继的两个地址处于同一个物理网上。不严格源路由选择：要求数据报必须沿着规定的 IP 地址序列传送，但是允许表中相继两个网址之间跳过多个网格。

时间戳选项：在源站点生成的一个空表，并由处理该数据报的路由器在表中填入该路由器的 IP 地址以及一个 32 位时间戳。

由于 IP 地址空间即将耗尽，以及新的 Internet 应用需要高效传输。现在正在进行 IPv4 到 IPv6 的转换。IPv6 保留了 IPv4 的许多优点，并进行了许多改进。IPv6 的特点主要有：扩大了地址空间，从原来的 32 位扩展到 128 位；简化了 IPv4 的报头格式，定义了服务质量，支持自动配置和重新编号等功能。

3.4.2 TCP 与 UDP 协议

1. 传输控制协议(Transmission Control Protocol，TCP)

TCP 协议是一个传输控制的协议，向下屏蔽了 IP 协议不可靠的传输的特性，向上提供可靠的点到点的传输。一般用于广域网。

(1) TCP 简介

TCP 协议提供面向连接的流传输，即数据传送前，主机间必须建立连接，传送完毕则需要拆除连接，TCP 提供从丢失或损坏数据中恢复报文和控制数据传输速度的功能。TCP 也包括根据网络状态调整到最佳性能的机制。首先来了解端口和 socket 地址。

① 端口

客户必须标识要到达的服务器，这可由指定服务器主机的 IP 地址和 TCP 端口号来完成。0～1023 端口号为公认著名端口，用于访问标准服务。用户应用程序只能使用大于 1023 的端口号。

常用协议对应的著名端口如表 3-2 所示。

表 3-2 常用协议对应的著名端口

端口号	用　　途	端口号	用　　途
9	丢弃所有新来的数据	53	域名系统区域传送
19	交换数据流	80	Web 服务器(HTTP)端口
20	FTP-DATA 文件传送数据端口	103	X400(用于 X400 邮件服务)
21	FTP 文件传送对话端口	110	POP3(用于 PC 邮件服务)
23	TELNET(远程登录)端口	139	NetBIOS 会话服务
25	SMTP 简单邮件传送协议端口		

② socket 地址

用户通信的 IP 地址和端口的结合为 socket 地址。

(2) TCP 协议的功能

① 确保 IP 数据报的成功传递。

② 对程序发送的大块数据进行分段和重组。

③ 确保正确排序以及按顺序传递分段的数据。

④ 通过计算校验和，进行传输数据的完整性检查。

TCP 是基于两个网络主机之间的端对端通信。TCP 从高层协议接收需要传送的字节流，将字节流分成段，然后 TCP 对段编号和排序以便传递。

（3）TCP 协议报文结构

TCP 协议报文结构如图 3-9 所示。

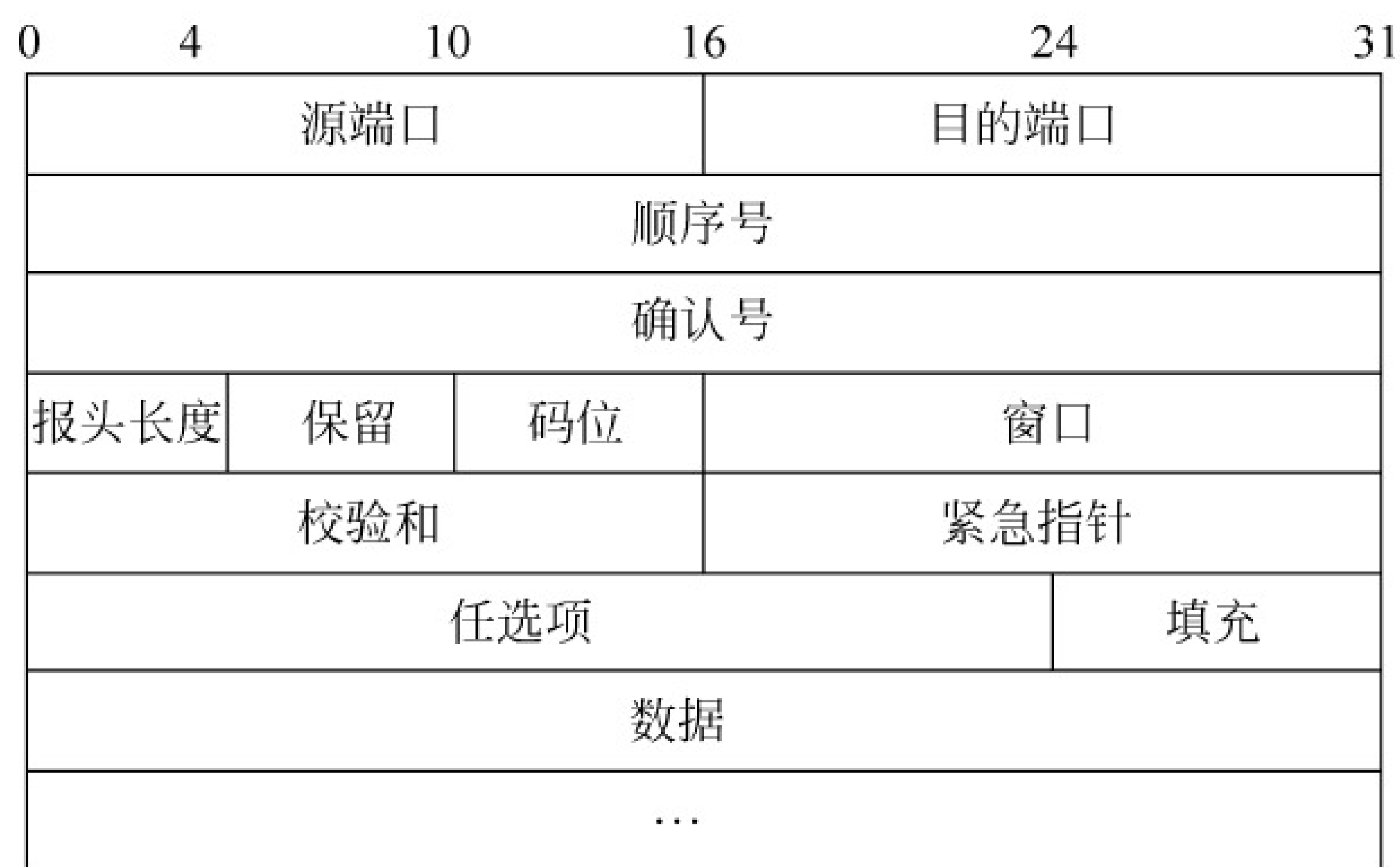


图 3-9　TCP 协议报文结构

（4）TCP 工作原理

TCP 经过一个连接建立、数据传输和连接释放的过程来实现可靠的数据传输。在两个 TCP 主机交换数据之前，必须先建立会话。TCP 会话通过三次握手的过程初始化。一旦初始的三次握手完成，在发送和接收主机之间按顺序发送和确认报文段。关闭连接之前 TCP 使用与建立连接类似的握手过程验证两个主机都完成发送和接收全部数据。

① 建立连接

两台主机应用程序间的连接必须建立在交换数据之前。连接的建立需要多次交换报文，其连接过程为三次握手。TCP 连接建立过程如图 3-10 所示。

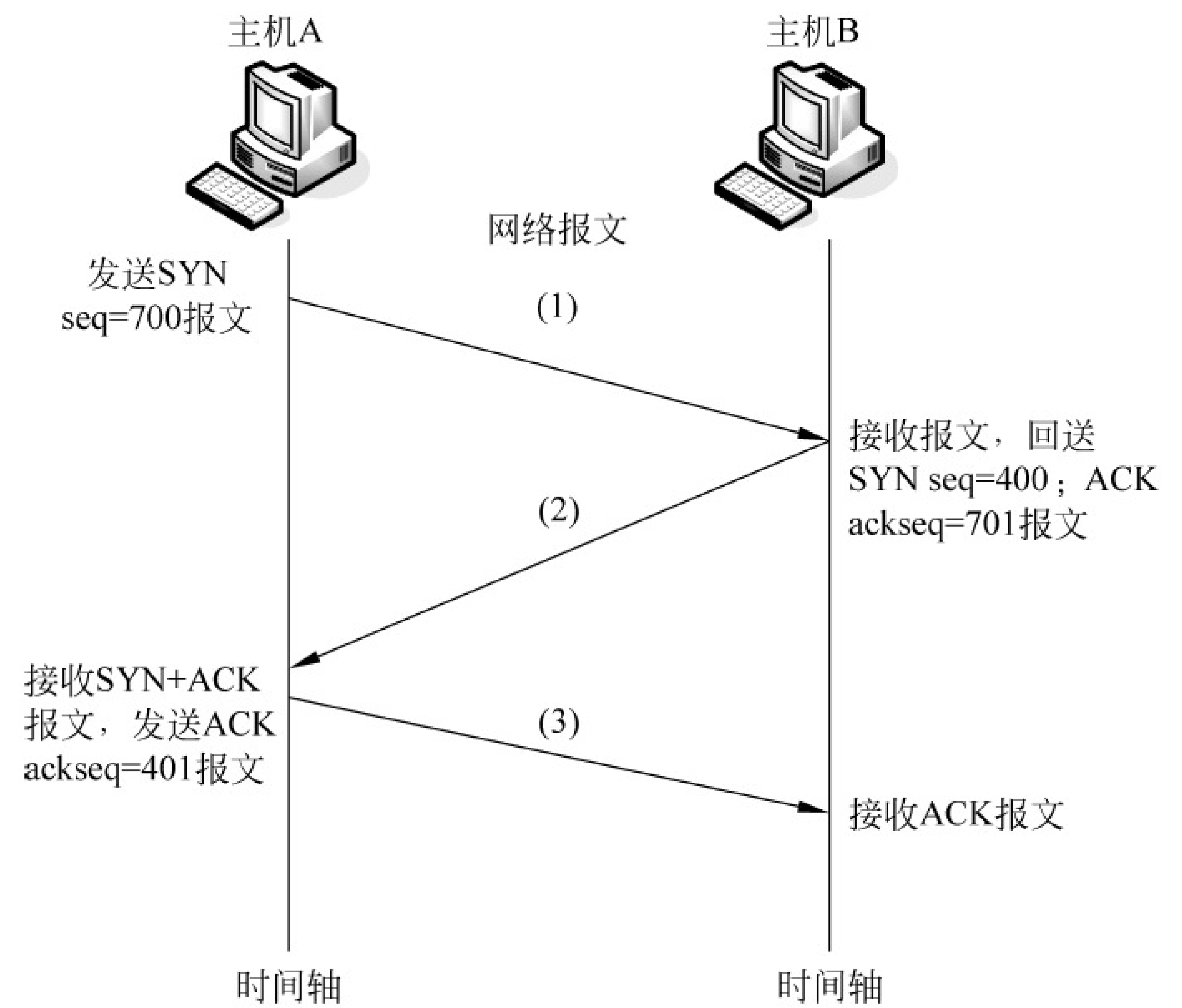


图 3-10　TCP 连接建立过程

a）主机 A 发送一主动建立命令告诉 TCP，A 启动 TCP 进程发送一初始序列号（如 700）的报文：SYN seq＝700。

b）当 SYN 到达时，主机 B 的 TCP 进程选择一初始序号（如 400），并根据主机 A 的 SYN 产生应答信息 ACK＝701，主机 B 给主机 A 回送报文：SYN seq＝400，ACK ackseq＝701。

c）当主机 A 的 TCP 接收到服务器的 SYN＋ACK 报文时，回送 ACK ackseq＝401 的报文。

d）主机 B 接收后，连接建立。

② 连接拆除（如图 3-11 所示）

a）主机 A 完成其工作，告诉 TCP 拆除连接；TCP 发送一 FIN 报文，通知对方没有更多数据要发送。

b）主机 B 接收并确认 FIN 报文；回送 ACK 报文。

c）主机 B 的 TCP 通知其应用程序，服务器要求拆除连接；客户告诉其 TCP 拆除连接；客户 TCP 发送一 FIN 报文。

d）主机 A 接收到客户的 FIN 报文，使用 ACK 来响应。

e）主机 A 通知其应用程序连接已拆除。

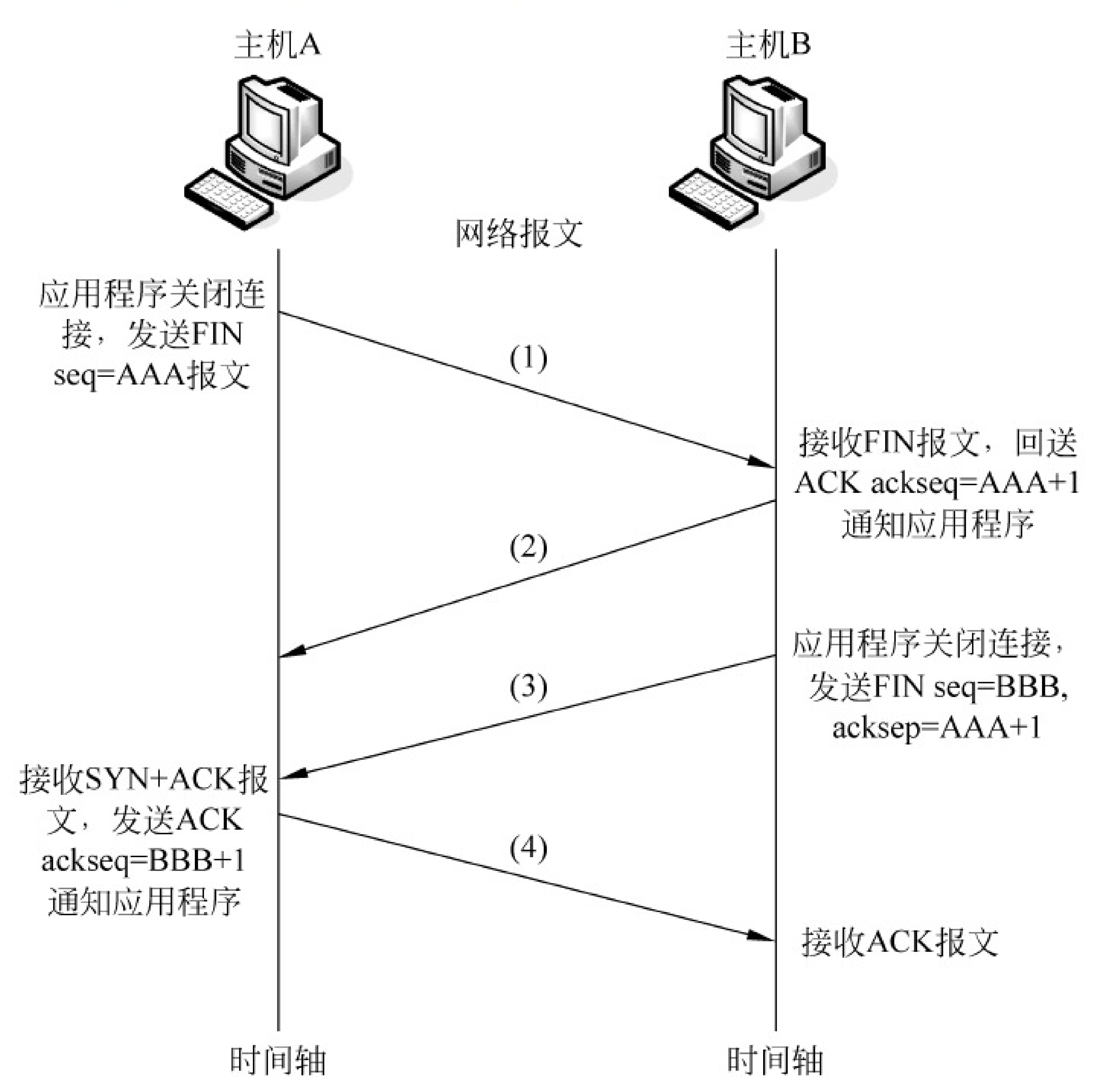


图 3-11　TCP 连接拆除

意外拆除连接由发送“重新建立”给对方来实现，通过设置 TCP 段头中的 RST 位来完成。

③ 最大段尺寸

以太网的最大数据报尺寸为 1500 字节。

2. 用户数据报协议(User Datagram Protocol,UDP)

TCP/IP 协议集中的传输层协议有数据传输协议 TCP 和用户数据报协议 UDP 两种。TCP 协议是专门为了在不可靠的互联网上提供一个可靠的端到端字节流而设计的。UDP 协议则支持无连接的传输,提供了一种方法来发送经过封装的 IP 数据报,而且不必建立连接就可以发送这些 IP 数据报。UDP 协议的报文格式如图 3-12 所示。

0	16	31
UDP源端口	UDP目的端口	
UDP报文长度	UDP校验和	
数据		
…		

图 3-12　UDP 协议的报文格式

UDP 协议的几个特性如下。

(1) UDP 是一个无连接协议,传输数据之前源端和终端不建立连接,当它想传送时就简单地去抓取来自应用程序的数据,并尽可能快地把它扔到网络上。在发送端,UDP 传送数据的速度仅仅受应用程序生成数据的速度、计算机的能力和传输带宽的限制;在接收端,UDP 把每个消息段放在队列中,应用程序每次从队列中读一个消息段。

(2) 由于传输数据不建立连接,因此,也就不需要维护连接状态,包括收发状态等,因此一台服务器可同时向多个客户机传输相同的消息。

(3) UDP 信息包的标题很短,只有 8 个字节,相对于 TCP 的 20 个字节信息包的额外开销很小。

(4) 吞吐量不受拥挤控制算法的调节,只受应用软件生成数据的速率、传输带宽、源端和终端主机性能的限制。

UDP 协议和 TCP 协议的主要区别是两者在如何实现信息的可靠传递方面不同。TCP 协议中包含了专门的传递保证机制,当数据接收方收到发送方传来的信息时,会自动向发送方发出确认消息;发送方只有在接收到该确认消息之后才继续传送其他信息,否则将一直等待直到收到确认信息为止。

与 TCP 协议不同,UDP 协议并不提供数据传送的保证机制。如果在从发送方到接收方的传递过程中出现数据报的丢失,协议本身并不能做出任何检测或提示。因此,通常人们把 UDP 协议称为不可靠的传输协议。

相对于 TCP 协议,UDP 协议的另外一个不同之处在于如何接收突发性的多个数据报。不同于 TCP 协议,UDP 协议并不能确保数据的发送和接收顺序。

虽然 UDP 协议是一种不可靠的网络协议,但由于 UDP 协议排除了信息可靠传递机制,将安全和排序等功能移交给上层应用来完成,极大地降低了执行时间,使速度得到了保证。例如,在屏幕上报告股票市场、在屏幕上显示航空信息以及实时通信等领域得到广泛应用。

3.4.3　其他常用协议

1. 远程登录协议(Telnet)

Telnet 协议是用来登录到远程计算机上,并进行信息访问,通过它可以访问所有的数据库、联机游戏、对话服务以及电子公告牌,如同与被访问的计算机在同一房间中工作一样,但只能进行些字符类操作和会话。

2. 文件传输协议(FTP)

文件传输协议是文件传输的基本协议,有了 FTP 协议就可以把文件进行上传,也可从网上得到许多应用程序和信息(下载),有许多软件站点就是通过 FTP 协议来为用户提供下载任务的,俗称“FTP 服务器”。最初的 FTP 程序是工作在 UNIX 系统下的,而目前的许多 FTP 程序是工作在 Windows 系统下的。FTP 程序除了完成文件的传送之外,还答应用户建立与远程计算机的连接,登录到远程计算机上,并可在远程计算机上的目录间移动。

3. 简单邮件传输协议(SMTP)

SMTP 协议是 TCP/IP 协议族的一个成员,这种协议认为你的计算机是永久连接在 Internet 上的,而且认为你在网络上的计算机在任何时候都是可以被访问的。它适用于永久连接在 Internet 的计算机,但无法使用通过 SLIP/PPP 协议连接的用户接收电子邮件。解决这个问题的办法是在邮件计算机上同时运行 SMTP 协议和 POP 协议的程序,SMTP 协议负责邮件的发送和在邮件计算机上的分拣和存储,POP 协议负责将邮件通过 SLIP/PPP 协议连接传送到用户计算机上。

任务完成:

大家都熟知的 QQ 聊天,发送方 QQ 写入的信息是最原始的,也就是应用层的工作;首先需要在传输层进行编码,而表示层则决定是用什么编码传输数据,有可能还包括加密的过程。会话层负责建立与对方的 QQ 应用程序建立会话。

在传输层通过 UDP 协议(为了保证数据的完整性也会用到 TCP 协议)通过双方应用程序即 QQ 进程的端口建立端到端的连接,而实际的数据的传递要通过 OSI 参考模型的最下边的三层进行。

网络层给数据包写上 IP 地址指明数据传输的目的地。在网络层进行寻址,确定传输的方向,即下一步该往哪儿走。数据链路层是在网络层封装的基础上封装 MAC 地址——网卡的物理地址,这样数据帧才能到达目的计算机。最后物理层就是原始的比特流传输,传输二进制“0”和“1”。

对方计算机的网卡检测到数据帧的 MAC 地址与自身的匹配,于是接收信息。经网络层与传输层的校验确认,最终来到应用层,转换成有意义的信息显示在对方的 QQ 程序窗口中。

知识拓展——OSI参考模型与TCP/IP参考模型的比较

通过前面的学习讨论,大家已经看到 TCP/IP 参考模型和 ISO/OSI 参考模型有许多相似之处。例如,两种参考模型中都包含能提供可靠的进程之间端到端传输服务的传输层,而在传输层之上是面向用户应用的传输服务。

尽管 ISO/OSI 参考模型和 TCP/IP 参考模型基本类似,但是它们还是有许多不同之处。在这里,将讨论两种参考模型的不同之处。有一点需要特别指出:是比较两种参考模型的差异,并不对两个参考模型中所使用的协议进行比较。

在 ISO/OSI 参考模型中,有三个基本概念:服务、接口和协议。也许 ISO/OSI 参考

模型的最重要的贡献是将这三个概念区分清楚了。每一层都为其上层提供服务,服务的概念描述了该层所做的工作,并不涉及服务的实现以及上层实体如何访问的问题。

层间接口描述了高层实体如何访问低层实体提供的服务。接口定义了服务访问所需的参数和期望的结果。接口仍然不涉及某层实体的内部机制,而只有不同机器同层实体使用的对等进程才涉及层实体的实现问题。只要能够完成它必须提供的功能,对等层之间可以采用任何协议。如果愿意,对等层实体可以任意更换协议而不影响高层软件。

上述思想也非常符合现代的面向对象的程序设计思想。一个对象(如模型中的某一层),有一组它的外部进程可以使用的操作。这些操作的语义定义了对象所能提供的服务的集合。对象的内部编码和协议对外是不可见的,也与对象的外部世界无关。

TCP/IP 参考模型并不十分清晰地区分服务、接口和协议这些概念。相比 TCP/IP 参考模型,ISO/OSI 参考模型中的协议具有更好的隐蔽性并更容易被替换。

ISO/OSI 参考模型是在其协议被开发之前设计出来的。一方面,意味着 ISO/OSI 参考模型并不是基于某个特定的协议集而设计的,因而它更具有通用性;另一方面,也意味着 ISO/OSI 参考模型在协议实现方面存在某些不足。

而 TCP/IP 参考模型正好相反。先有协议,参考模型只是现有协议的描述,因而协议与参考模型非常吻合。问题在于 TCP/IP 参考模型不适合其他协议栈。因此,它在描述其他非 TCP/IP 网络时用处不大。

下面来看看两种参考模型的具体差异。其中显而易见的差异是两种参考模型的层数不一样:

ISO/OSI 参考模型有 7 层,而 TCP/IP 参考模型只有 4 层。两者都有网络层、传输层和应用层,但其他层是不同的。两者的另外一个差别是有关服务类型方面。ISO/OSI 参考模型的网络层提供面向连接和无连接两种服务,而传输层只提供面向连接服务。TCP/IP参考模型在网络层只提供无连接服务,但在传输层却提供两种服务。

综上所述,使用 ISO/OSI 参考模型(去掉会话层和表示层)可以很好地讨论计算机网络,但是 OSI 协议并未流行。TCP/IP 参考模型正好相反,其模型本身实际上并不存在,只是对现存协议的一个归纳和总结,但 TCP/IP 协议却被广泛使用。

实训 3　简单协议的实现

1. 实训目的

编程实现客户机/服务器通信。

2. 实训内容

在 TCP/IP 协议网络中两个进程间的相互作用的主机模式是客户机/服务器模式(Client/Server model)。该模式的建立基于以下两点:①非对等作用;②通信完全是异步的。两个节点间的通信必须用协议来实现,在网络编程领域,使用 socket 技术是最重要的一种方式。此处给出一个简单的示例,让读者了解协议的实现过程。

客户机/服务器模式在操作过程中采取的是主动请示方式(通信程序如图 3-13 所示)。

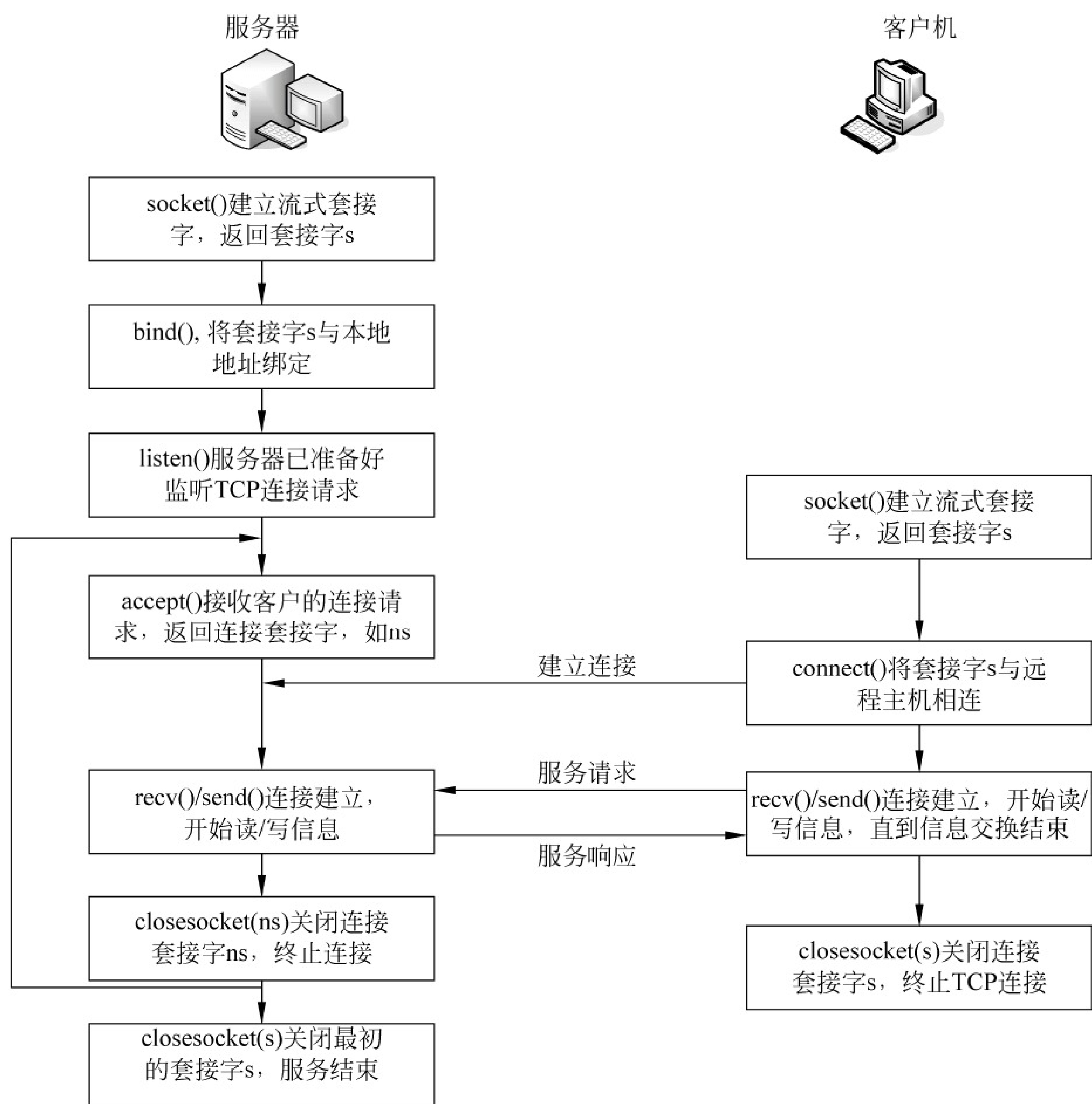


图 3-13　面向连接的 socket 通信程序

首先服务器方要先启动，并根据请示提供相应服务：

（1）打开一通信通道并告知本地主机，它愿意在某一个公认地址上接收客户请求。

（2）等待客户请求到达该端口。

（3）接收到重复服务请求，处理该请求并发送应答信号。

（4）返回第(2)步，等待另一客户请求。

（5）关闭服务器。

客户方：

（1）打开一通信通道，并连接到服务器所在主机的特定端口。

（2）向服务器发送服务请求报文，等待并接收应答；继续提出请求。

（3）请求结束后关闭通信通道并终止。

3. 实训步骤

（1）根据图 3-13 所示，分析客户机与服务器的交互过程。

（2）用 C 语言编写利用 socket 通信的程序代码，实现简单字符的传输。

(3) 编译、调试。

4. 实训要求

(1) 对编写程序进行本地和网络测试。

(2) 写出调试过程中遇到的问题与解决方法。

习　题　3

1. 选择题

(1) 完成路径选择功能是在 OSI 参考模型的(　　)。

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 传输层

(2) 关于网络体系结构,以下(　　)描述是错误的。

A. 物理层完成比特流的传输

B. 数据链路层用于保证端到端数据的正确传输

C. 网络层为分组通过通信子网选择适合的传输路径

D. 应用层处于参考模型的最高层

(3) 负责提供可靠的端到端数据传输的是(　　)的功能。

A. 传输层　　B. 网络层　　C. 应用层　　D. 数据链路层

(4) 下列功能中,属于表示层提供的是(　　)。

A. 交互管理　　B. 透明传输　　C. 死锁处理　　D. 文本压缩

(5) 下列说法错误的是(　　)。

A. TCP 协议可以提供可靠的数据流传输服务

B. TCP 协议可以提供面向连接的数据流传输服务

C. TCP 协议可以提供全双工的数据流传输服务

D. TCP 协议可以提供面向非连接的数据流传输服务

2. 填空题

(1) 在 TCP/IP 协议族中,运输层的________ 提供了一种可靠的数据流服务。

(2) 在 OSI 参数模型中,处于数据链路层与传输层之间的是________层。

(3) 在 OSI 网络体系结构中,________为分组通过通信子网选择适合的传输路径。

3. 简答题

(1) 什么是计算机网络的体系结构?

(2) 两个最著名的计算机网络体系结构是什么? 它们发展的结果如何?

(3) TCP/IP 协议实现网络互联的关键思想是什么?

(4) 简述 OSI 计算机网络体系结构各层的主要功能。

模块 4　组建局域网

任务 4.1　组建小型局域网

任务描述：在家庭或者办公室里，有两台或两台以上的计算机，就有通过网络互联实现资源共享的需求。所谓麻雀虽小，五脏俱全，两台计算机之间的互联通信属于网络构建的问题，这涉及传输介质的选择，网络设备的安装以及通信协议的配置等知识。接下来通过学习局域网的知识来找到解决方案。

任务分解为：

子任务一：完成双机互联网络的组建；子任务二：完成用集线器组建局域网。

4.1.1　网络硬件

1. 局域网的基本概念

局域网(Local Area Network，LAN)是一种在一个局部区域范围(例如一个学校、一个工厂、一家医院、一个机关等)内，把各种计算机、外部设备、数据库等互联起来组成的计算机通信网。

区别于一般的广域网，局域网通常具有如下特征。

(1) 地理分布范围小。一般为数百米至数千米，可以覆盖一幢大楼、一所学校或者一个企业。局域网一般为一个机构所拥有。

(2) 数据传输速率高。一般为 10Mbps～10Gbps，可以交换各类数字和非数字(如语音、图像、视频等)信息。

(3) 误码率低。这是因为局域网通常采用短距离基带传输，可以使用高质量的传输媒体，从而提高了数据传输质量。

(4) 以个人计算机为主体。包括各种终端及外部设备，网络中一般不设中央主机系统。

(5) 一般仅包含 OSI 参考模型中的下层功能，即仅涉及通信子网的内容。所以联入局域网的数据通信设备必须加上高层协议和网络软件才能组成计算机网络。

(6) 协议简单，结构灵活，建网成本低，周期短，便于管理和扩充。

2. 局域网的组成

一般来讲，局域网是由计算机、传输介质、网卡、LAN 连接设备、网络操作系统和局域网应用软件组成。

局域网上的计算机又可分为服务器和工作站两类。局域网的连接设备包括介质的连接器件、集线器、交换机等。

按局域网的体系结构可以分为工作站/文件服务器结构、客户机/服务器结构和对等网结构。

（1）局域网传输介质

常见的网络传输介质可分为两类：一类是有线传输介质；一类是无线传输介质。有线传输介质主要有双绞线、同轴电缆和光纤；无线传输介质有微波、无线电、激光和红外线等。各种传输介质的特性在模块 2 中已经进行了详细的介绍，这里不再重复。

（2）网络适配器

网络适配器即网络接口卡（Network Interface Card，NIC），简称网卡，图 4-1 显示的是 PCI（Peripheral Component Interconnect）接口的网卡。网卡是实现计算机互联的重要设备，在局域网系统中，互联起来的每个端设备上都有网卡，其作用是为工作站与网络间提供数据传输的功能，为工作站与网络建立逻辑和物理链路。在 OSI 参考模型中，网卡属于数据链路层的设备。

网卡的主要功能如下：

① 数据转换。由于数据在计算机内是并行传输，而在计算机之间是串行传输，所以网卡要实现数据的串并转化。具体来讲就是网卡可以进行数据帧的封装与拆解。

② 数据缓存。由于在网络系统中，工作站与服务器对数据的处理速率通常是不一样的，为了防止数据在传输过程中丢失，实现对数据传输的控制，网卡设有数据缓冲存储器对数据进行缓存。

③ 通信服务。网卡可以实现 OSI 参考模型的任何一层的通信协议，但在多数情况下，网卡提供的通信协议服务是在物理层和数据链路层上的。这些通信协议软件通常被固化在网卡内的只读存储器中。

根据不同的需要，网卡有多种不同的型号。按照网卡接口总线类型来分，有 ISA 总线网卡，例如 NE-2000 等；有 PCI 总线的网卡，例如 NE-550 等。一般 PCI 总线的比 ISA 总线的要快。如没有特殊限制的话，推荐最好选用 PCI 总线的网卡，而且这种网卡在进行网络配置时也相对容易一些。

按照工作速度又可分为 10Mbps 网卡、100Mbps 网卡、10/100Mbps 自适应网卡和 1000Mbps 网卡等。

另外，还有专门为笔记本电脑设计的专用网卡 PCMCIA（如图 4-2 所示），以及随着近几年来无线局域网技术而产生的无线局域网网卡。

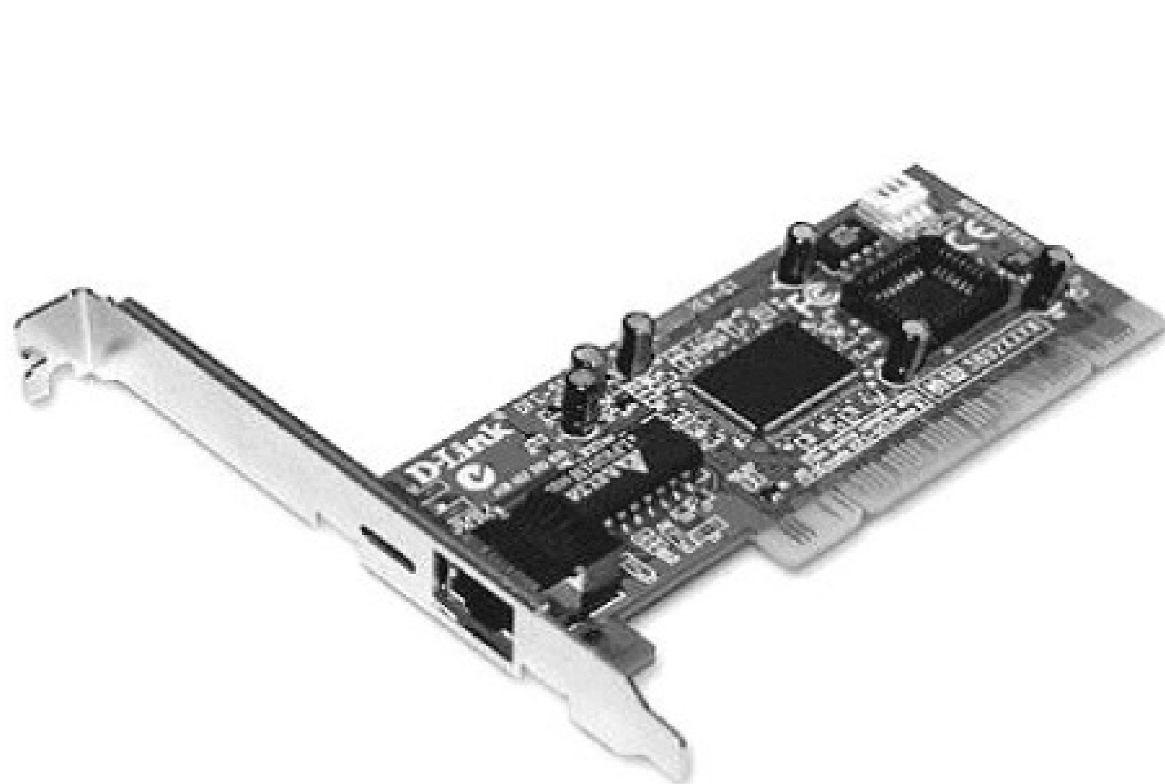


图 4-1　PCI 网卡



图 4-2　笔记本电脑网卡 PCMCIA

(3) 网络服务器

在网络系统中,网络服务器负责管理系统的共享设备,同时负责提供数据和文件管理、打印、通信等标准化服务。服务器是局域网中的核心设备,负责部分或全部网络的运行和数据的控制管理。

服务器为网上的其他计算机提供服务,一个局域网中至少有一台服务器,一般稍微复杂的局域网,都配有多台服务器。例如文件服务器、打印服务器、数据库服务器、通信服务器、应用程序服务器和事务处理服务器等。大量的网络软件主要驻留在服务器上,因而,局域网的功能主要由服务器来实现,它的性能好坏直接影响整个局域网。建成后的服务器都需要一定的通信处理能力、快速的访问应答能力和安全容错能力。

常用服务器及其功能如下。

文件服务器是整个网络系统的核心,提供网络用户管理、网络资源管理和网络安全管理等常用的服务。一般由网络操作系统以及相应的服务程序和一台专门运行这些程序的计算机组成。文件服务器对计算机的性能要求很高,要有比较大的硬盘空间和内存、足够的网络接口等,以满足各种网络服务的需要。

打印服务器用于管理和控制网络共享打印服务,一方面,负责从网络工作站中接收到打印的数据,并将这些数据放到打印队列中;另一方面,在打印服务器上按打印队列选取打印作业送到网络打印机。通常网络打印机要直接连接到打印服务器上,单个用户也可以将本地打印机设置成网络共享打印机。

通信服务器是一个专用系统,为网络上需要通过远程通信链路传送文件或访问远地系统或网络上信息的用户提供通信服务。通信服务器根据软件和硬件能力为一个或同时为多个用户提供通信信道。通常有异步远程网桥(SRB)、远程存取服务器(NAS)和异步通信服务器(NACS)。

(4) 用户工作站

工作站也叫客户机,是网络的前端窗口,是局域网上的各种用户和终端设备的通称,用户通过运行前端的应用程序来获得网络服务器的服务,并访问网络服务器中的共享资源。在局域网中,工作站可由计算机担任,也可由输入/输出终端担任。工作站通过插在扩展槽中的网卡经过传输介质连接到网络服务器上。

根据实际需求,工作站可以带有光盘、硬盘,也可以没有这些设备。前者称为有盘工作站,后者称为无盘工作站。无盘工作站成本低,有部分的防病毒功效,但加重了服务器的处理负担;有盘工作站设有磁盘驱动器,使用方便。

工作站与终端的差异:工作站本身应该是具有独立处理能力的完整的计算机,可以独立工作也可以连到网络中工作;终端则是人—机对话的设备,通常用于小型机等多用户系统中,它同工作站一样可以完成很多功能,不要混淆两者。

3. 局域网的拓扑结构

局域网的拓扑结构主要是总线型结构、环型结构和星型结构,因此,可以把局域网分为总线型局域网、环型局域网、星型局域网和混合型局域网等类型。

选择局域网拓扑结构需要考虑以下因素。

(1) 易于安装与扩展。

(2) 具有高可靠性,易于诊断故障和隔离。

(3) 与相应的访问控制方法相结合,选择合适的传输媒介,提高节点运行速度,降低复杂性。

4. 以太网

局域网发展到今天已经十分普及了,在各种局域网中,以太网的应用最为广泛。以太网最早是由美国 Xerox(施乐)公司创建的,1980 年,DEC、Intel 和 Xerox 三家公司联合提出了以太网规范。

(1) 传统以太网

传统以太网即标准以太网,是指运行速率为 10Mbps 的以太网。虽然今天的以太网已经发展到快速以太网、千兆以太网、万兆以太网,但是它们的基本工作原理都是从传统以太网发展而来的。因此,学习传统以太网的工作原理仍然是学习其他新型网络技术的基础。下面以目前使用最广泛的 10Base-T 以太网为例进行介绍。

(2) 双绞线 10Base-T 以太网

双绞线 10Base-T 以太网是使用非屏蔽双绞线为传输介质,并且在网络拓扑结构中增加了集线器 Hub 连接总线型结构(如图 4-3 所示),是星型和总线型结合的网络结构。

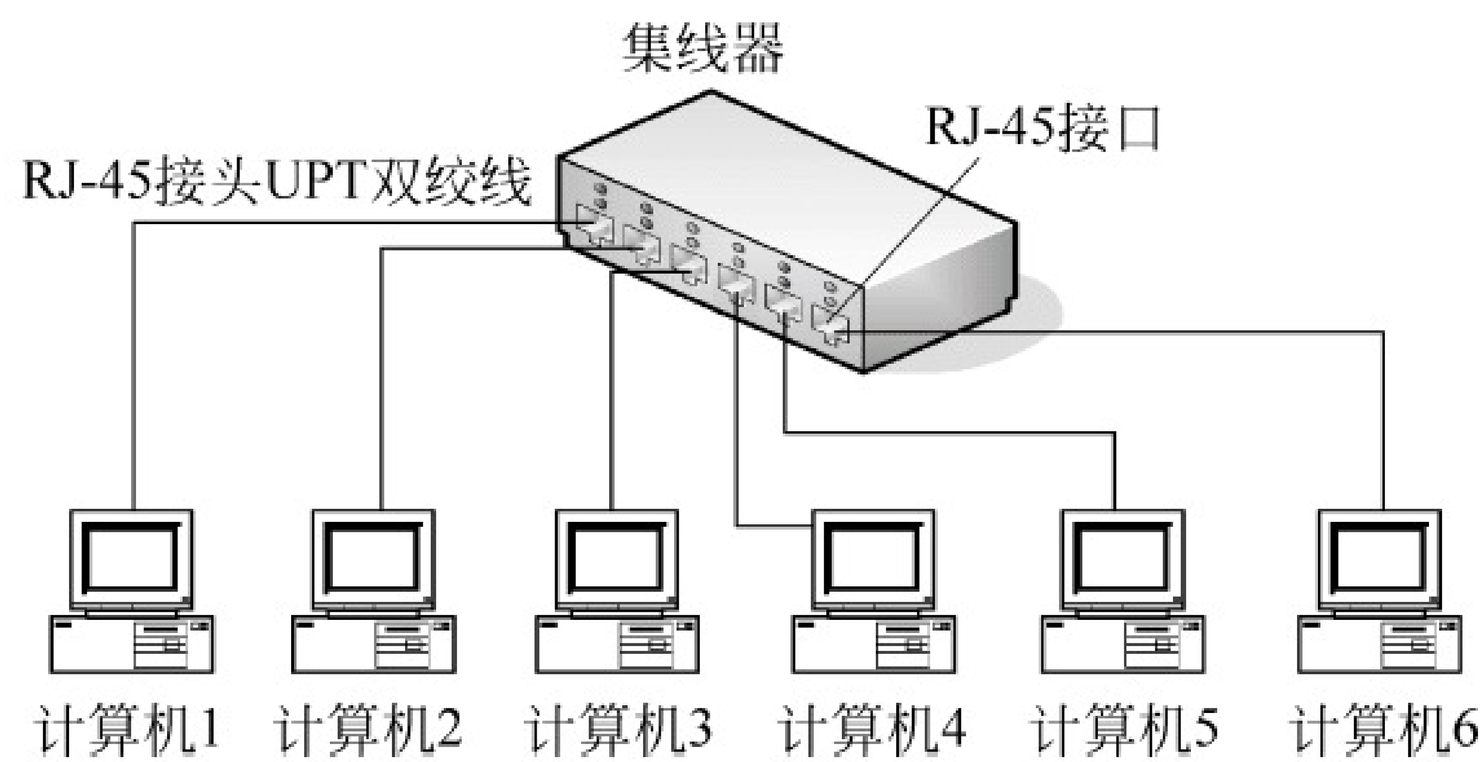


图 4-3　10Base-T 以太网

10Base-T 以太网的基本硬件设备是:

① 带有 RJ-45 接口的 Ethernet 网卡。

② 集线器 Hub。

③ 三类以上非屏蔽双绞线。

④ RJ-45 连接头。

⑤ 中继器。

10Base-T 以太网中工作站通过集线器 Hub 联入网络中,也可以直接联入网络;Hub 与各工作站之间采用双绞线作为传输介质,通过 RJ-45 标准接口连接。

以下是一个标准 10Base-T 以太网的主要性能指标:

① 使用非屏蔽双绞线连接收发器与集线器以及集线器与工作站,收发器与集线器间的距离不能超过 100m。

② 一个集线器能够连接多达 24 个工作站。

③ 一个中心集线器能够连接多达 12 个以上集线器进行网络扩展。

④ 无须使用网桥在网络上可连接多达 1023 个工作站。

由于粗缆 10Base-5 以太网与细缆 10Base-2 以太网引起性能和维护上的不足，已经逐渐淡出应用，所以此处不再介绍。

随着网络的发展，传统标准的以太网技术已经不能满足日益增长的网络数据流量的需求。快速以太网技术应运而生，如 100Mbps 快速以太网技术 100Base-TX，100Base-T4 和 100Base-FX 等技术标准。其中 100Base-TX 技术几乎是在 10Base-T 的基础上进行的直接升级，使用 5 类非屏蔽双绞线达到了 100Mbps 的数据传输速率，得以普遍使用。此外，千兆位以太网 1000Base-SX，1000Base-LX 和 1000Base-CX 等技术标准也相继制定出来。

以光纤为传输介质的 10Gbps 以太网技术也在研发中，但由于与当前的传输介质不兼容，还不能普及使用。

子任务一：双机互联网络的组建。

两台计算机的直接连接可以使用网卡和双绞线的连接方式，也可以通过串口使用电缆直接连接。采用第一种方法，在每台计算机上安装一块网卡，然后制作一条交叉连接的非屏蔽双绞线，直接将双绞线和计算机中的网卡连接即可。

1. 硬件连接

(1) 制作双绞线

根据网线的使用场合，制作网线。如计算机连接集线器、计算机连接交换机时，采用直接连接法——即两端都采用 EIA/TIA 568B 标准或 EIA/TIA 568A 标准。如同种设备连接，采用交叉连接法——即一端采用 EIA/TIA 568B 标准，另一端采用 EIA/TIA 568A 标准。确定好网线的制作方法后，使用制作网线的工具完成网线的制作并进行连通性的测试。

(2) 安装网卡

台式机安装步骤如下：

① 关闭计算机电源，打开机箱。

② 在计算机的主板上选择一个扩展槽，将网卡用力插入插槽，并将网卡固定。

③ 装好机箱盖，将 UTP 双绞线的 RJ-45 连接头插入网卡上的插口内，接通计算机电源。

2. 安装和配置协议

安装好 Windows XP 操作系统后，在“网络连接”窗口中，有一个“本地连接”图标。右击建立的本地连接，配置它们的 IP 地址和子网掩码。设两台计算机的 IP 地址分别是 192.168.10.1 和 192.168.10.2，子网掩码都是 255.255.255.0，配置完成后单击“确定”按钮，所配置的静态 IP 地址生效。

3. 网络连接状态的测试

局域网安装和配置完成后，在默认状态下，在任务栏的右侧会显示一个局域网连接状态的图标。鼠标停留在此图标上，会显示连接状态信息。要查看详细的连接状态信息，单击图标，可以看到网络连接的持续时间、速度、发送和接收的数据量等信息。

右击本地连接图标，可以对连接禁用。若网线未插入，图标的两台计算机显示为断开状态。

4. 连通性测试

运行“CMD”,在 DOS 联机状态下,可以通过 ping 命令来确认配置了 TCP/IP 的计算机能否正常工作。

(1) ping 127.0.0.1。用于确认 TCP/IP 是否被正确加载。若失败,必须检查 TCP/IP 协议的安装。

(2) ping 192.168.0.1 或 ping 192.168.0.2。用于确认 IP 地址是否被正确加载,并检查 IP 地址是否与网络中其他计算机发生冲突。

(3) ping 网络上另外一台计算机的 IP 地址。用于测试网络的连通状况。

4.1.2　局域网的体系结构与协议

1. 局域网的体系结构

局域网的体系结构与 OSI 参考模型相比,只具有相当于 OSI 参考模型的最低两层。因为局域网不存在路由选择问题,所以局域网没有网络层。但是物理连接以及位流在介质上的传输都是必需的,所以具有相当于 OSI 参考模型的物理层与数据链路层。

由于局域网的种类繁多,其介质接入、传输控制的方法各有不同,为了使局域网中的数据链路层不至于过于复杂,将局域网的数据链路层进行了分层,分为逻辑链路控制子层 LLC 和介质访问控制子层 MAC。局域网的体系结构如图 4-4 所示。

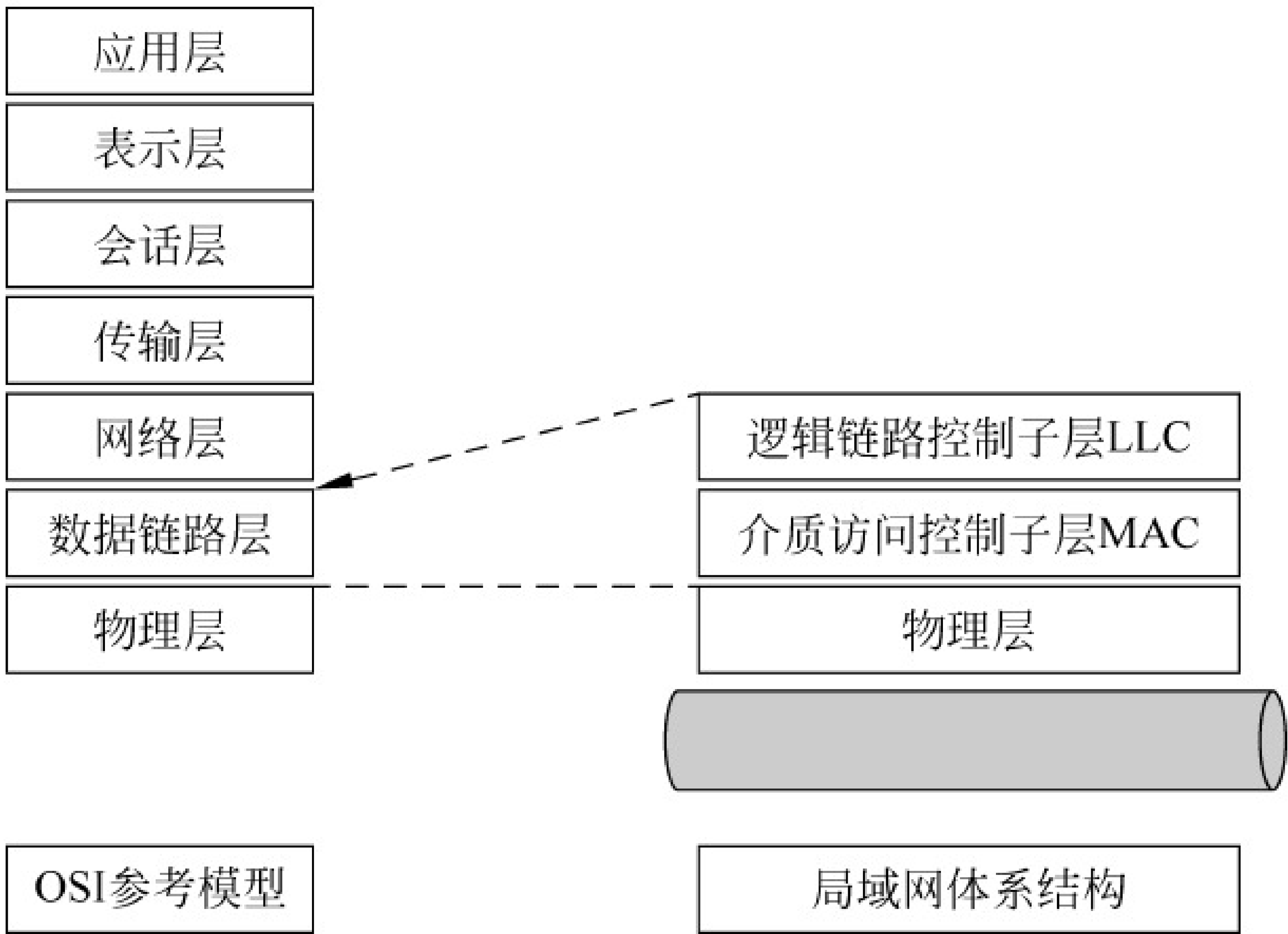


图 4-4　局域网体系结构与 OSI 参考模型

(1) 物理层的功能:物理层规定了信号的编码形式,多使用曼彻斯特编码;规定了传输信号的介质,主要为双绞线、同轴电缆和光纤等。物理层还规定局域网以总线型、星型和环型为主的拓扑结构;数据传输速率分为 1Mbps、4Mbps、10Mbps、100Mbps 等。简单讲物理层的功能在于实现位流的传输与接收、同步前序的产生与删除等。

(2) 介质访问控制子层(MAC)的主要功能是:

① 数据帧的操作,包括发送时将上层下来的数据封装成帧,以及接收后将帧拆解传到上层。

② 实现和维护 MAC 协议。

③ 数据流的差错检测。

④ 寻址。

(3) 逻辑链路控制子层 (LLC)的主要功能是:

① 逻辑链路的操作,包括数据链路层逻辑连接的建立与释放。

② 提供与高层的接口。

③ 差错控制。

④ 数据帧的排序。

2. 局域网的协议标准

IEEE 802 委员会于 1980 年开始研究局域网标准,1985 年公布的 IEEE 802 标准被 ISO 作为局域网的国际标准,后又扩充了多项标准文本。

IEEE 802 标准系列包含以下部分:

IEEE 802.1A 概述和系统结构、IEEE 802.1B 寻址、网络管理和网际互联。

IEEE 802.2 逻辑链路控制。

IEEE 802.3 CSMA/CD 总线访问控制方法及物理层技术规范。

IEEE 802.4 令牌总线访问控制方法及物理层规范。

IEEE 802.5 令牌环网访问控制方法及物理层规范。

IEEE 802.6 城域网访问控制方法及物理层技术规范。

IEEE 802.7 宽带技术。

IEEE 802.8 光纤技术(FDDI 在 IEEE802.3、IEEE802.4、IEEE802.5 中的使用)。

IEEE 802.9 综合业务数字网(ISDN)技术。

IEEE 802.10 局域网安全技术。

IEEE 802.11 无线局域网。

IEEE 802.12 新型高速局域网(100Mbps)。

3. 介质访问控制方法

(1) IEEE 802.3 的总线访问控制方法——CSMA/CD

IEEE 802.3 定义了带冲突检测的载波侦听多路访问(Carrier Sense Multiple Access With Collision Detection,CSMA/CD)方法。CSMA/CD 是采用争用技术的一种介质访问控制方法。可将 CSMA/CD 形象地概况为用先听后发/边听边发的方法来共享传输介质。CSMA/CD 的工作原理如下(如图 4-5 所示):

① 假如介质是空闲的,则发送。

② 如介质忙,则继续侦听,直到介质空闲,立即发送。

③ 若在发送过程中检测到冲突发生,则立即停止发送,并向总线上发一串阻塞信号,通知总线上各站冲突已发生。这样可避免因白白传送已损坏的帧而浪费信道容量。如果在最大往返传播延迟时间内没有冲突,则停止冲突检测。

④ 冲突发生后,发送一串阻塞信号,按照二进制退避算法确定一随机时间,等待时间过后,再重新尝试发送。

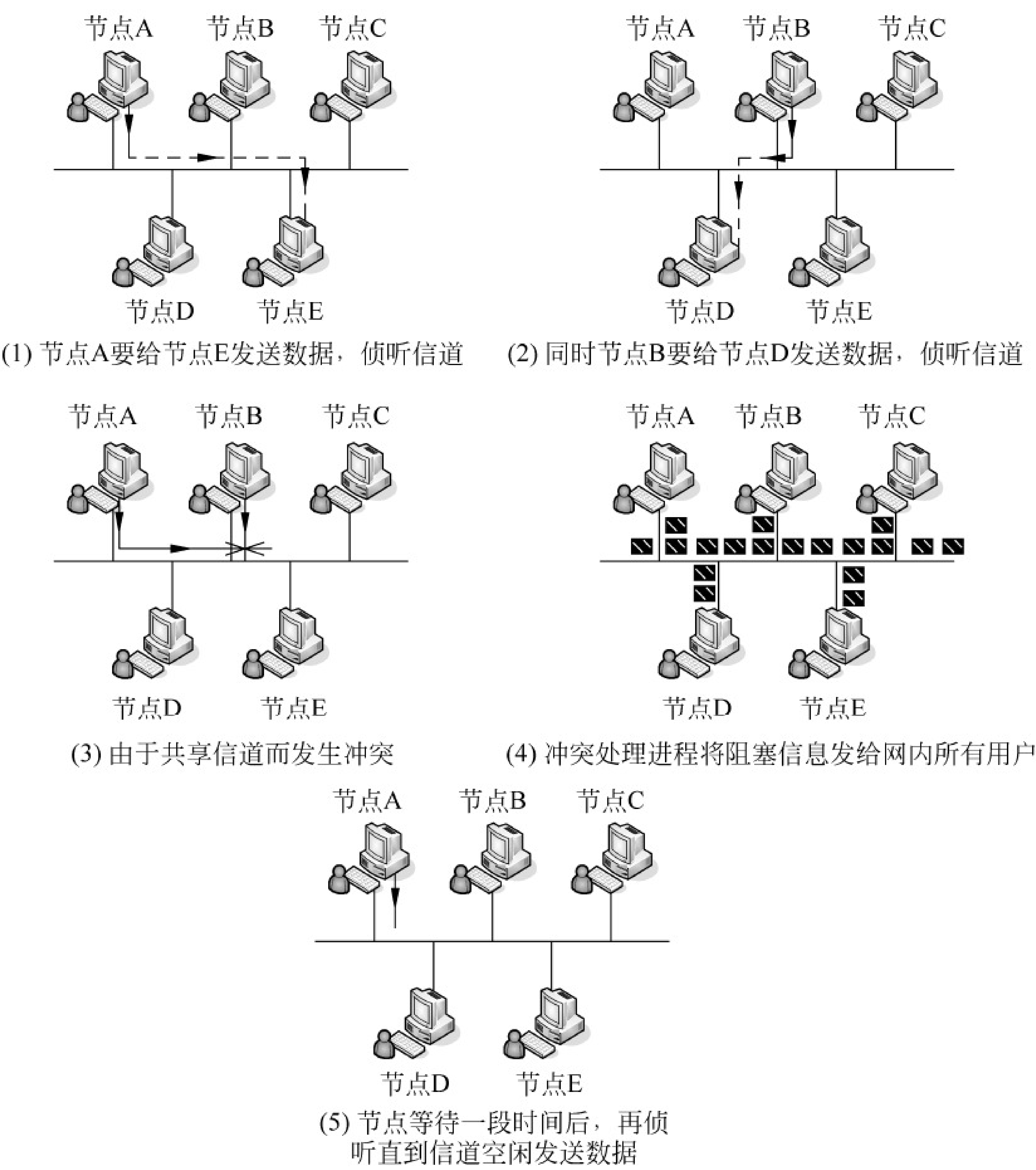


图 4-5 CSMA/CD 工作原理

图 4-6 描述了 CSMA/CD 的工作流程。

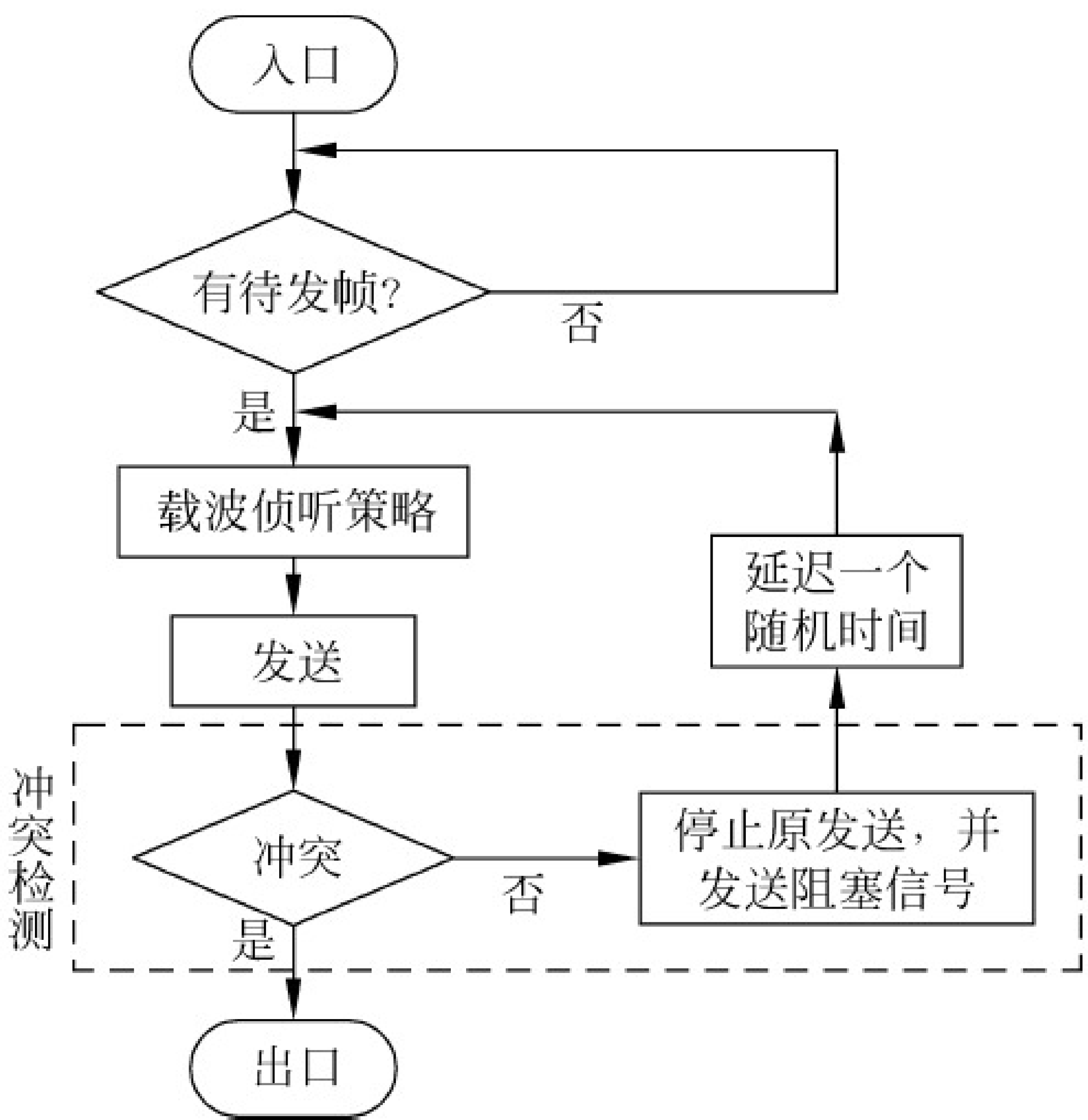


图 4-6 CSMA/CD 工作流程

(2) IEEE 802.5 的令牌环网访问控制方法——Token Ring

令牌环原理是采用"令牌"传递机制,令牌是一段简短的报文,绕环传输。当它不带入信息时叫做空令牌或自由令牌(Free Token)。需要发送信息的计算机首先捕获令牌,在令牌被捕获期,其他计算机不得发送数据,捕获到令牌的计算机修改令牌,加进数据和源、目的地址,然后把令牌发送上环,这时的令牌叫"忙令牌",目标机收到忙令牌后下载信息,再把令牌还给发送者,当发信者再次收到令牌后,知道数据已到达目的地,将令牌信息清空。令牌重获"自由身",又开始绕环传输,直到下一个要发送的计算机捕获它。如果没有要发送信息的计算机,空牌就一直循环。IBM 令牌环网就是这样工作的。

(3) IEEE 802.4 的令牌总线访问控制方法——Token Bus

令牌总线访问控制是在物理总线上建立一个逻辑环,令牌在逻辑环路中的传递原理与令牌环相同。它既具有总线网的接入方便和可靠性高的优点,也具有令牌环网的无冲突和发送时确定的上限值的优点。

子任务二:用集线器组建局域网。

将两台以上的计算机组建成局域网,计算机数量较少时,可以采用一台集线器组网。若网络中的计算机数量较多,可以采用两台以上的集线器级联结构组网或堆叠式集线器结构组网。

1. 集线器的选购

根据计算机的数量和机房情况,选择集线器的类型(桌面型集线器,端口数量较少,适用于中小型办公网络环境;机架结构的集线器端口数量较多,通常安装在机柜中或机架上)、选择端口数(一般是 8 的倍数;为了便于网络扩容,要选择提供 Uplink 级联端口)、端口带宽(10Mbps 一般用于数据传输量要求较低的家庭组网中;100Mbps 用于数据传输量较大的中型网络;10/100Mbps 自动匹配集线器是目前应用最为广泛的一种,同时适用于 100Base-TX 和 10Base-T 两种网络环境)。

2. 组建单一集线器局域网

采用 100Base-TX 标准组网,网络拓扑结构选择星型结构,首先在计算机中,安装 100Mbps 或 10/100Mbps 自适应的网卡,集线器选择 100Base-TX(端口为 RJ-45 插口),端口数一般不超过 16 口。双绞线选择 5 类 UTP,长度小于 100m,制作直通线。当网络中的硬件设备连接完毕后,在每台机器上安装相应的操作系统,配置 TCP/IP,测试网络的连通性。

3. 多集线器级联结构组网

集线器级联的方式有两种。

- 交叉线:用交叉双绞线连接两个集线器的普通端口,实现集线器的级联。
- 直通线:用直通双绞线连接一个集线器的上行端口(Uplink)和另外一个集线器的普通端口,实现集线器的级联。

任务 4.2　构建虚拟局域网

任务描述:新增的 5 个新计算机用户分别属于不同的部门,出于办公成本及技术上的考虑,单位的所有用户都连在一个交换机上。那么如何才能实现多用户数据传输的畅

通以及不同部门间的信息独立与安全呢？

任务分析：我们知道一个交换机所连接的网络为一个物理网段，属于同一个广播域。该网段的广播数据可以被网段内的任何用户接收，在不增加物理设备的情况下如何才能将一个大的广播域分段呢？下面来学习虚拟局域网的相关知识。

4.2.1　虚拟局域网基础

在同一局域网(LAN)网段内的所有节点通过集线器、网桥或交换机等设备连接起来，形成了一个广播域。其中各节点之间可以直接通信，而处于不同局域网段内的设备之间的通信则必须经过路由器转发。

随着网络的不断扩展，接入设备逐渐增多，网络结构也日趋复杂。局域网规模的增大导致广播信息的剧增，甚至形成广播风暴导致网络拥塞。而如果用更多的路由器划分广播域，不仅会增加运行成本，而且会使网络时延加长，从而导致网络数据传输速度的下降。

另外，将所有用户放在同一个网段也会带来安全与管理上的问题，如同一局域网内的用户，可以窃听到其他用户的传输等。

所以较好的做法是把需要经常联系的用户划分在一个局域网中(这样他们之间就可以通过网桥连接，而无须通过路由器)，然后把需要分开的组划分到不同的局域网中(这样每个组都不会受到其他组的广播包的影响)。这就是虚拟局域网的基本思想。

虚拟局域网(Virtual Local Area Network，VLAN)是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的新型技术。VLAN 所连接的设备可以来自不同的物理网段，但是相互之间可以进行直接通信，好像处于同一网段中一样。而不同 VLAN 间的通信需要路由设备的转发。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域，即 VLAN。每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个工作站无须被放置在同一个物理空间，即这些工作站不一定属于同一个物理网段。一个 VLAN 内部的广播和单播流量都不会转发到其他的 VLAN 中，从而有助于控制流量，减少设备投资，简化网络管理，提高网络安全性。

4.2.2　构建虚拟局域网

虚拟局域网通常用一个 VLAN 号(VLAN ID)和 VLAN 名(VLAN Name)标识(如图 4-7 所示)。多个交换机之间的虚拟局域网通过 VLAN 标记以及虚拟网中继(VLAN Trunk)技术实现。

划分 VLAN 是通过使用软件定义 VLAN 成员实现的。定义 VLAN 成员的方法主要有三种：基于端口划分 VLAN、基于 MAC 地址划分 VLAN 和基于第三层协议类型或地址划分。

1. 基于端口划分 VLAN

基于端口划分 VLAN 就是按交换机端口定义 VLAN 成员，每个端口只能属于一个 VLAN，这是一种通用的方法。利用交换机的端口来划分 VLAN 成员，被设定的端口都在

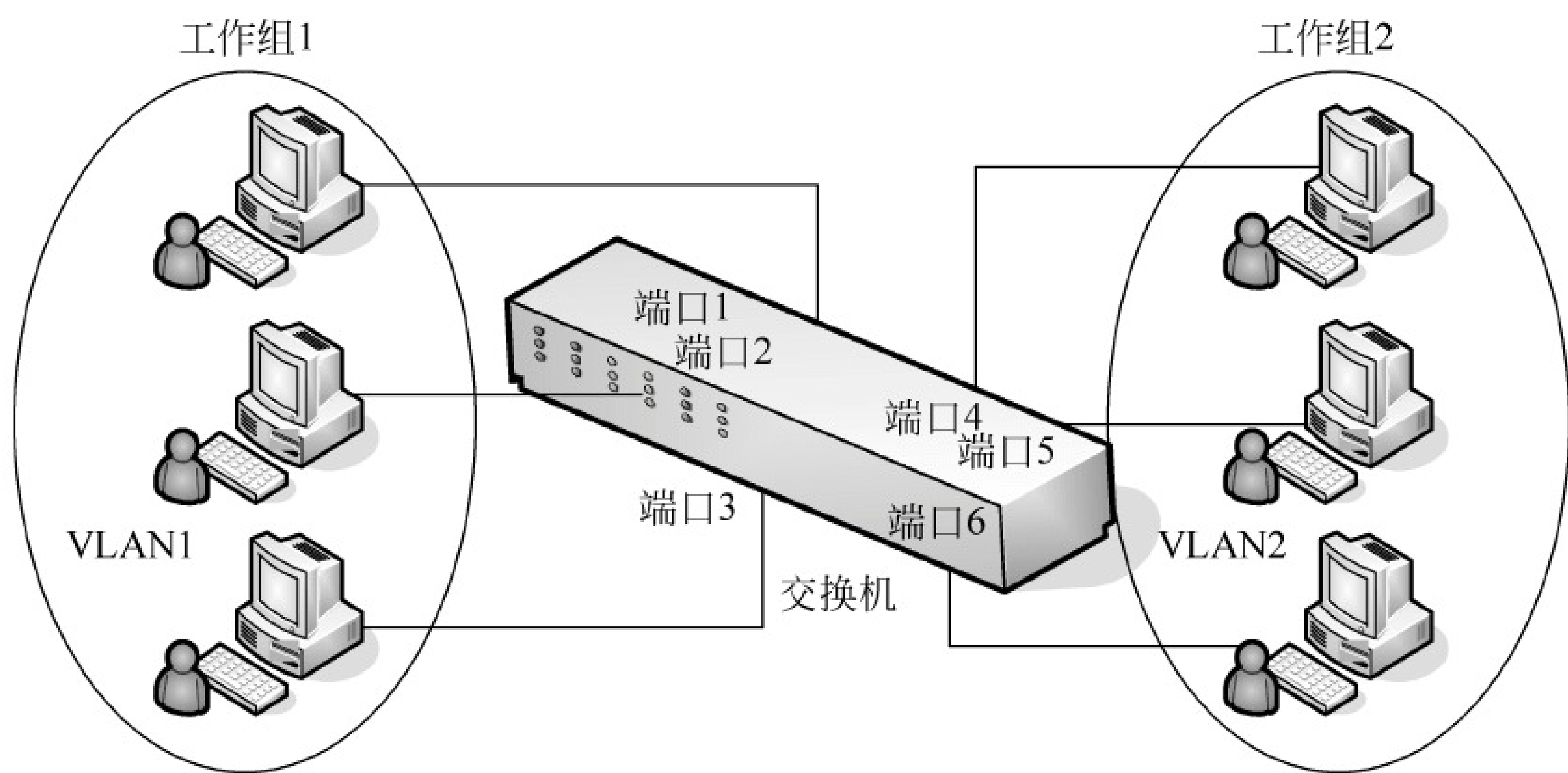


图 4-7 VLAN 划分示意图

同一个广播域中。例如,一个交换机的 1、2、3、4、5 端口被定义为虚拟网 AAA,同一交换机的 6、7、8 端口组成虚拟网 BBB。这样做允许各端口之间的通信,并允许共享型网络的升级。但是,这种划分模式将虚拟局域网限制在了一台交换机上。第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN,不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员,其配置过程简单明了。因此,从目前来看,这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。这种方式是静态配置方式,容易实现和监视,比较安全。

2. 基于 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分,即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时,即从一个交换机换到其他的交换机时,VLAN 不用重新配置,所以,可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种方法的缺点是初始化时,所有的用户都必须进行配置,如果有几百个甚至上千个用户的话,配置是非常烦琐的。而且这种划分的方法也导致了交换机执行效率的降低,因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员,这样就无法限制广播包了。另外,对于使用笔记本电脑的用户来说,他们的网卡可能经常更换,这样 VLAN 就必须不停地配置。

3. 基于第三层协议类型或地址划分

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的,虽然这种划分方法是根据网络地址,比如 IP 地址,但它不是路由,与网络层的路由毫无关系。

这种方法的优点是用户的物理位置改变了,不需要重新配置所属的 VLAN,而且可以根据协议类型来划分 VLAN,这对网络管理者来说很重要,另外,这种方法不需要附加的帧标记来识别 VLAN,这样可以减少网络的通信量。

这种方法的缺点是效率低,因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头,需要更高的技术,同时也更费时。

任务实现：

要实现不同部门用户的分组，需要在交换机上使用配置命令，建立对应不同部门的不同 VLAN，最简单的方式就是将交换机的端口分配给不同的 VLAN。此处以简单的 VLAN 实验说明局域网的划分及应用。

以交换机为中心正确连接网络中的各个设备，如图 4-8 所示：用户计算机 PC1～PC6 对应交换机的端口 1～端口 6 使用直通双绞线相连。在没有任何设置的情况下，这 6 台计算机可以相互通信，并且可以接收到彼此的广播信息。处于某种需要，要把 PC1～PC3 3 台计算机与 PC4～PC6 3 台计算机进行隔离，在不改变当前连接状态的情况下，使两部分不能直接通信，无法接收彼此的广播信息。这就用到虚拟局域网技术。如前所述，划分虚拟局域网有多种方式，此处以基于交换机端口划分为例。

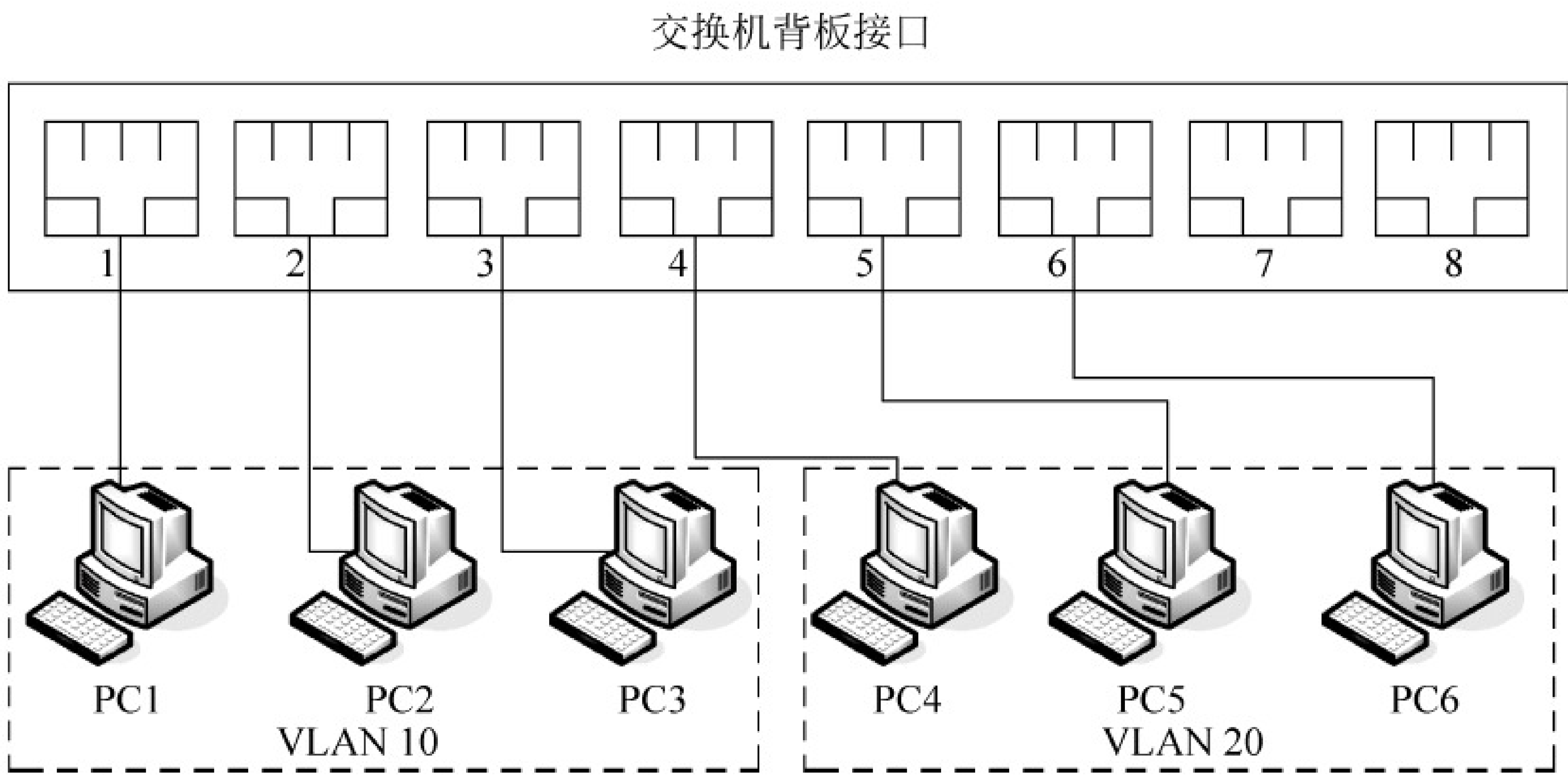


图 4-8　虚拟局域网划分

(1) 初始状态如图 4-8 所示，给 PC1～PC6 分别配置 IP 地址如下：

```
PC1: 192.168.10.1;PC2: 192.168.10.2;PC3: 192.168.10.3;PC4: 192.168.10.4;PC5: 192.168.10.5;
PC6: 192.168.10.6.
```

在任意计算机上使用 ping 命令测试与其他计算机的连通性，它们彼此是互通的。

(2) 进入交换机 IOS(Internet Operating System，网际操作系统) VLAN 配置模式，创建 VLAN 10 和 VLAN 20。将 f0/1 分配到 VLAN 10(注意不同厂商的交换机设备操作命令稍有不同，实际配置可参考设备说明)。

将 f0/2 和 f0/3 分配到 VLAN 20 中

```
switch# config terminal                          ; 进入全局模式
switch(VLAN) # VLAN 10                           ; 创建 VLAN 10
switch(VLAN) # no VLAN 2                         ; 删 VLAN 2
switch(config) # int f0/1                        ; 进入端口 1
switch(config-if) # switchport access VLAN 10    ; 当前端口 1 加入 VLAN 10
…
```

使用相同的方法将端口 2、3 加入到 VLAN 10 中；创建 VLAN 20，将端口 4、5、6 加入到 VLAN 20 中。

(3) 测试 PC1/PC2/PC3 与 PC4/PC5/PC6 的连通性,使用 ping 命令,如无法 ping 通,说明已经将两部分划分在了不同的虚拟局域网中。

知识拓展——组建无线局域网

随着 Internet 应用的迅猛发展,便携机、PDA(Personal Data Assistant)等移动智能终端为随时随处接入 Internet 提供了可能。无线网络的应用成为发展的必然。在接入速率和适应环境上与 3G 技术互为补充的 WLAN(Wireless Local Area Network),即无线局域网迅猛发展,成为新一代高速无线接入网络。图 4-9 描述了无线局域网的应用。

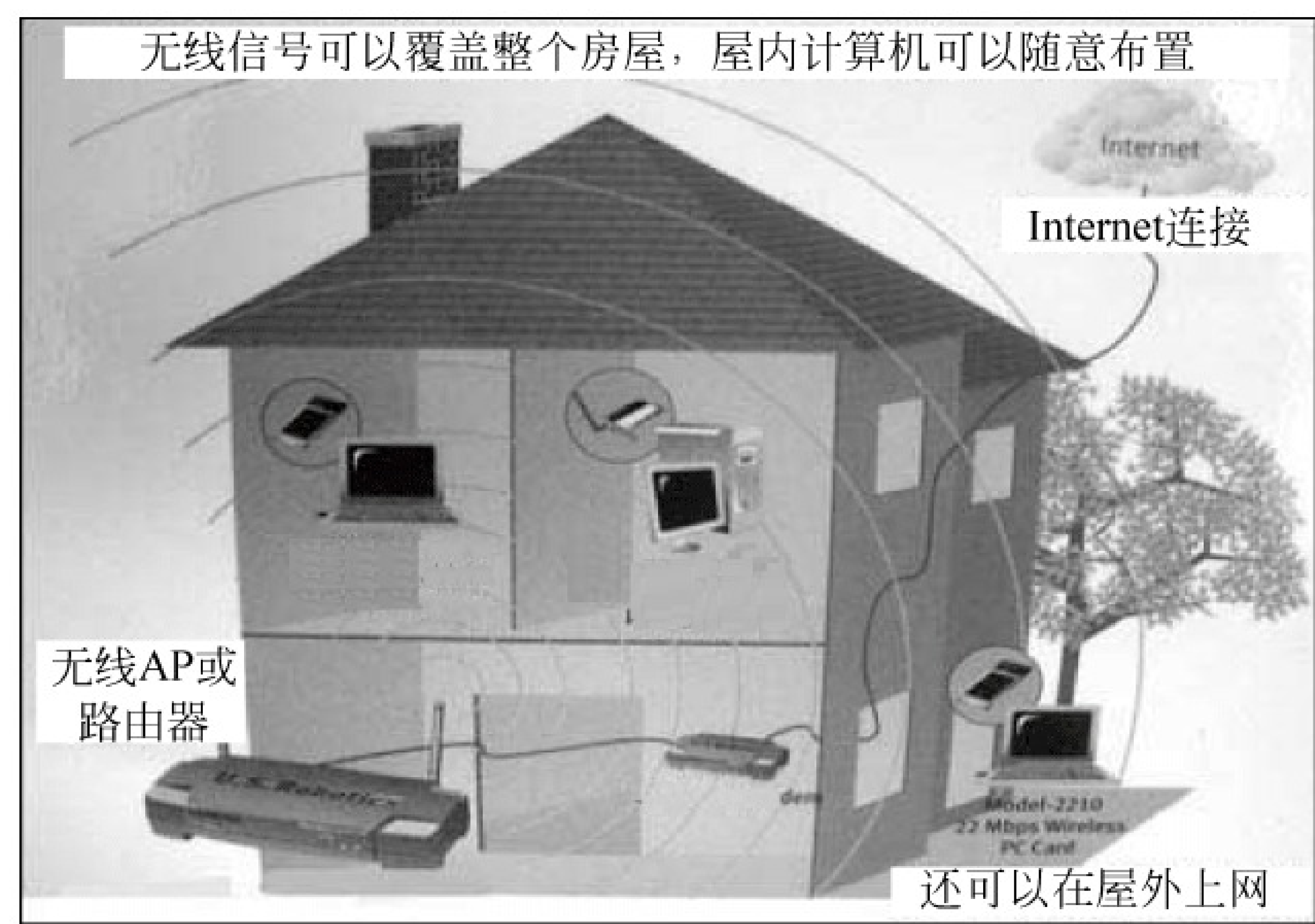


图 4-9　无线局域网

1. 无线局域网的标准

IEEE 802.11 是在 1997 年由大量的局域网以及计算机专家审定通过的标准。IEEE 802.11 规定了无线局域网在 2.4GHz 波段进行操作,这一波段被全球无线电法规定为扩频使用波段。

1999 年 8 月 IEEE802.11 标准得到了完善,其中 IEEE802.11b 标准的制定从根本上改变了 WLAN 的设计与应用状况。其数据速率最大可达 11Mbps,并可以根据情况的变化在不同速率间切换。目前,大多数厂商生产的 WLAN 产品都基于该标准。

2. 无线局域网的特点与应用

无线局域网作为有线网络的延伸与补充具有显著的优点:可移动性;设备安装快速、简单、灵活;无须布线,投资少;易扩展。

基于无线局域网的诸多优点,无线局域网的典型应用包括医院、学校、金融服务、制造业、服务业、公司应用、公共访问等。

3. 无线局域网的组建

组建无线局域网的无线网络设备主要包括:无线网卡、无线访问接入点、无线网桥和天线。

无线局域网的拓扑结构有两种:对等(Ad-hoc Network)网络和结构化(Infras-

tructure)网络。

对等网络是指网络中的用户通过无线网卡直接连接,不必使用接入点设备。几台计算机装入无线网卡,即可达到相互联接、资源共享的目的。但是,用户数量一般为 4～8 个,用户数较多时,网络性能较差,并且用户之间的有效通信距离约为 100m。该网络无法接入有线网络,只能独立使用。

(1) 组建小型工作组无线局域网。

选择无线网卡。每台计算机中安装一块支持 IEEE 802.11b 或 IEEE 802.11g 的无线网卡。选择硬件标准、品牌最好相同。目前市场上的无线网卡的接口有 USB 接口、PCI 接口或者笔记本电脑使用的 PCMCIA 接口。

配置无线网卡无线局域网的操作系统可以选用 Windows 2000。一般情况下,网卡会自动识别,网卡上的主要参数有:网络类型、无线网络的网络名称(Service Set IDentifier,SSID)、工作信道、IP 地址和子网掩码等。

配置步骤如下:

在控制面板中,找到无线网卡设置项。配置无线网卡,在配置文件名(Profile Name)中,输入一个文件名,如 XXGC1。在网络类型(Network Type)中,选择"对等式模式"(Ad-hoc)。在无线网络的网络名称中输入一个网络名称。对其他配置可以采用默认配置,完成后,单击"确定"按钮。

用 ping 命令进行连通性测试。

(2) 组建结构化的无线局域网。

结构化的无线局域网通常作为有线局域网的一种补充或扩展。网络中的 AP 保证了各个无线客户机之间的通信,扩展了用户之间的数据传输距离,而且无线用户可以访问有线网络上的打印机和服务器等设备。

结构化无线局域网如图 4-10 所示。

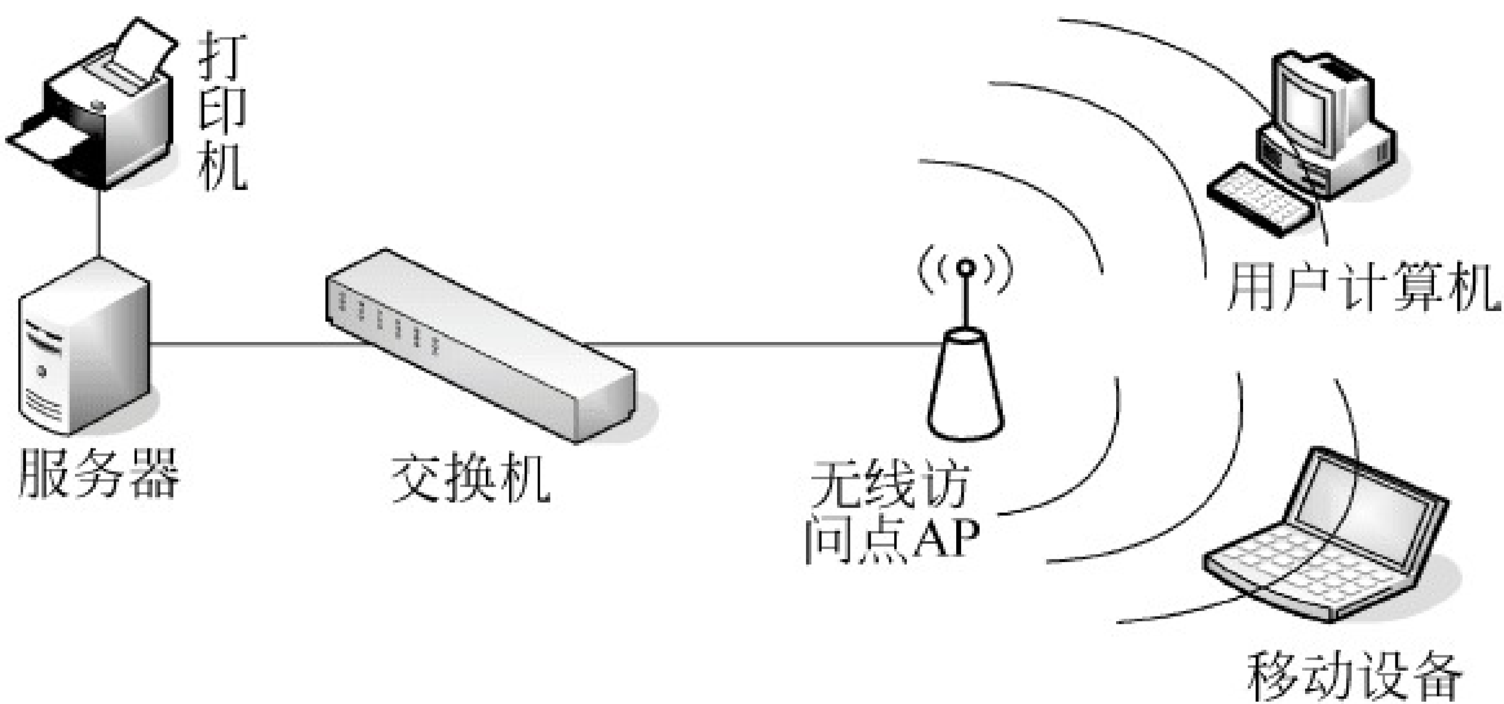


图 4-10　结构化无线局域网

安装步骤如下:

安装一个接入点设备,将接入点设备连接到网络设备(如集线器或交换机)后,在某一以太网客户机上安装接入点设备管理程序(AP Manager),配置接入点设备管理程序,在客户端上,运行接入点设备管理程序。

配置接入点设备的基本参数:接入点设备名(Access Point Name),为 AP 设置一个名字,如 XXGC-1;无线网络的网络名称(SSID),尽量不要使用默认名(Wireless),可以设

置为XXGC-1-Wireless；其他配置可以保持默认配置。

配置客户端的基本参数：设置配置文件名(如JSJ1)；在网络类型中选择“存取点”模式(Infrastructure Access Point)；在无线网络的网络名称(SSID)中输入和接入点设备的SSID一致的名称，否则网络不会连通；对其他配置可以采用默认配置。

设置TCP/IP，若存在DHCP服务器，可以设置为自动获取IP地址，若没有DHCP服务器，都要接入点无线设备和无线客户端设置为静态IP地址，且必须处于同一个网段。

实训4　组建微型局域网

1. 实训目的

组建宿舍局域网。

2. 实训内容

学校的校园网建设已非常普遍。随着学生计算机的普及，同学们上网的需求也越来越多。如何在寝室里组建一个微型局域网，成为目前同学们最想了解的问题。

3. 实训步骤

(1) 组网设备准备工作

首先，选购适合自己需要的宽带路由器。宽带路由器有两个作用，一个作用是连接不同的网络；另外一个作用是选择信息传递的线路。现在市面上的宽带路由器，价格已经大幅度下降，技术不断创新，DNS、QoS、防火墙、远程唤醒、时间管理等功能，配上大容量内存或者闪存能使路由器的数据处理能力更加如虎添翼。所以宽带路由器已经取代交换机成为构建微型局域网的首选设备。

如图4-11所示，TL-R402M SOHO宽带路由器是专为满足中小型企业办公和家庭上网需要而设计的，具有性能优越、配置简单的特点。提供多方面的管理功能，可对系统、DHCP服务器、虚拟服务器、DMZ主机、防火墙、上网权限管理、静态路由表、UPnP等进行管理，同时提供全中文配置界面，用户界面友好，配置简单易用。当然，市面上设备型号多种多样，可根据需要选择性价比最适合的型号。



图4-11　TL-R402M SOHO宽带路由器

(2) 选择组网方式

普通大学宿舍都是8人间的，但也有6人间和4人间的，宿舍与宿舍之间的距离一般都不会太远。总的来说，各高校的宿舍环境不尽相同，因此组网方案也应该因地制宜。如图4-12所示方案是大学宿舍里用得最多的，也是最为简单的。

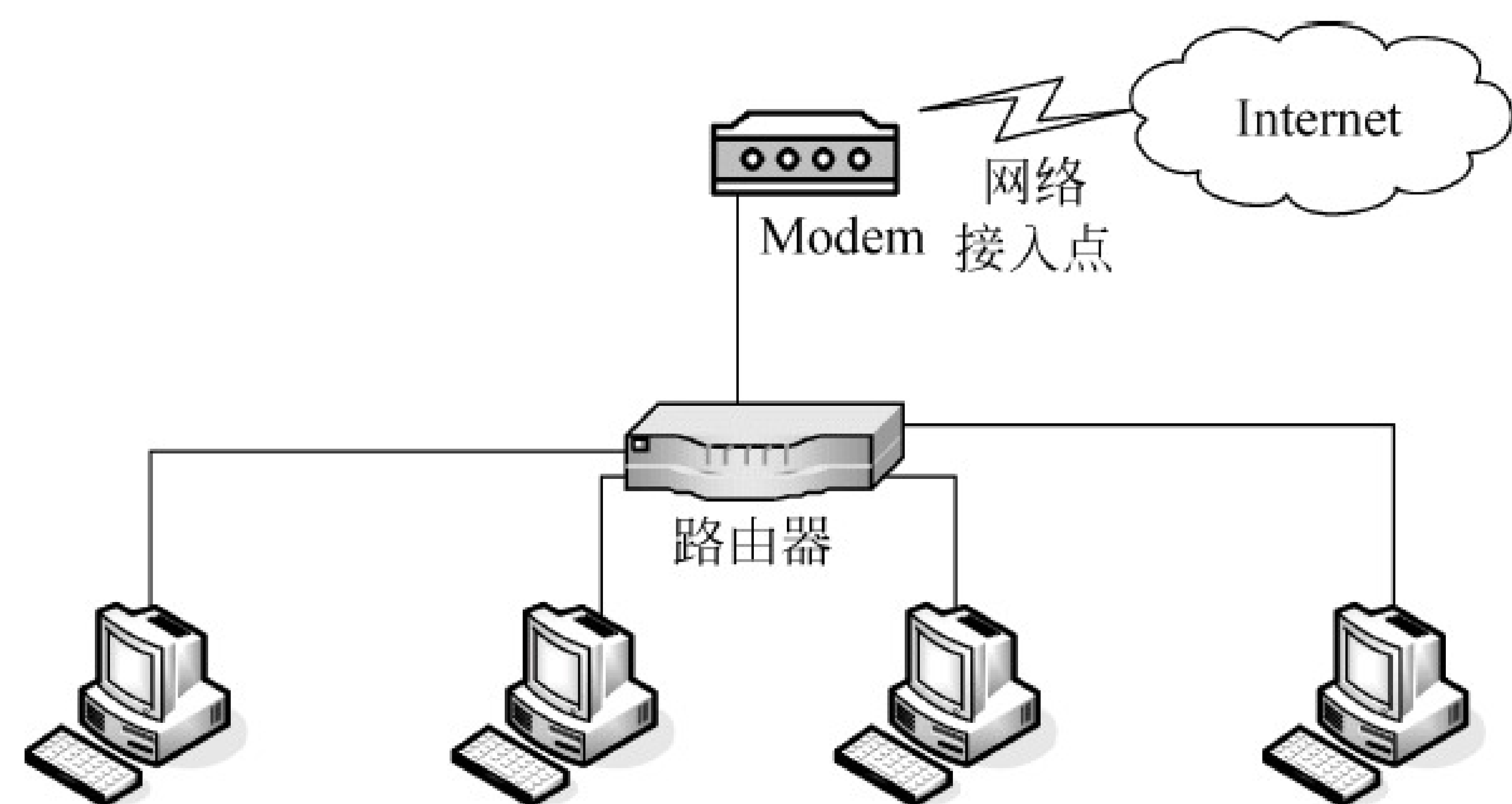


图 4-12　组网方案

路由器的价格大幅度下降，使集线器和交换机已经没有了生存的空间，加之路由器的设置简单好用，取代集线器和交换机是必然的趋势。用直通线把 Modem 和路由器接起来，客户机与路由器的连接则是用交叉线，然后进入路由器设置一下就可以轻松上网了。

（3）选择网线

双绞线由相互绞合在一起的线对组成，为制作网线时便于区分，每条线都标有不同的颜色。由于基于双绞线的星型拓扑比总线型拓扑更容易维护，所以双绞线成为目前组建局域网时最常用的一种线缆。按照前面介绍的双绞线的制作及测试方法完成网线的制作。

（4）选购与安装网卡

网卡（Network Interface Card）的作用是将数据分解为数据包再发送至网络。平时我们说的 10Mbps、100Mbps、1000Mbps 网卡都是按网卡连接速率来区分的，市面上的大多数网卡都是自适应的。网卡的安装与设置可参考前面相应章节。

（5）设备连接

用路由器来组建局域网是最简单、最方便、最快捷的。宽带路由器一般都提供了 4 个端口，具体的连接方式是：ADSL 宽带线路连接 ADSL Modem，直接双绞线连接 Modem 和路由器，其他计算机用交叉双绞线与路由器连接，如果计算机较多可考虑用交换机或集线器进行扩展。然后进行路由器的简单配置就能轻松上网冲浪了。

4．实训要求

（1）列出设备明细，画出网络拓扑图。

（2）分析宿舍局域网用到的协议。

习　题　4

1．选择题

（1）典型的局域网可以看成由以下三部分组成：网络服务器、工作站与（　　）。

A．IP 地址　　B．通信设备　　C．TCP/IP 协议　　D．网卡

（2）在计算机网络中，一方面连接局域网中的计算机；另一方面连接局域网中的传

输介质的部件是(　　)。

A. 双绞线　　B. 网卡　　C. 转发器　　D. 路由器

(3) 目前应用最广泛的一类局域网是 Ethernet。Ethernet 的核心技术是随机争用型介质访问控制方法,即(　　)。

A. Token Ring　　B. Token Bus　　C. CSMA/CD　　D. FDDI

(4) CSMA/CD 方法用来解决多点如何共享公用总线传输介质的问题,网中(　　)。

A. 不存在集中控制的节点　　B. 存在一个集中控制的节点

C. 存在多个集中控制的节点　　D. 可以有也可以没有集中控制的节点

(5) 决定局域网特性的主要技术要素包括(　　)、传输介质与介质访问控制方法。

A. 所使用的协议　　B. 网络拓扑结构

C. 数据传输环境　　D. 主机的时钟频率

2. 填空题

(1) 虚拟局域网用软件方式来实现逻辑工作组的划分与管理,其成员可以用交换机端口号、________或网络层地址进行定义。

(2) 局域网在网络拓扑上主要采用了环型、星型和________结构。

(3) 一般认为,决定局域网特性的主要技术有三种,它们是介质访问控制方法、传输介质和________。

(4) 在共享介质方式的总线型局域网实现技术中,需要利用________方法解决多节点访问共享总线的冲突问题。

(5) IEEE ________标准定义了 CSMA/CD 总线介质访问控制子层与物理层规范。

3. 简答题

(1) 试分析 CSMA/CD 介质访问控制技术的原理。

(2) 什么是 VLAN? 它有什么特点?

模块5　互联网的使用

任务5.1　配置 Windows XP 工作站

任务描述：Internet 将全世界的信息资源集合成一个整体。通过 Internet，人们可以了解世界各地的信息、下载文件、收发电子邮件、网上聊天、网上购物、观看影片等。要享受 Internet 提供的精彩服务，必须先接入 Internet。用户通过合理配置个人计算机的网络参数接入 Internet，就可以从 Internet 的应用中真正体会到“资源共享”的真正含义。

5.1.1　认识 Internet

1. Internet 概述

Internet 即国际计算机互联网，也叫因特网，是目前世界上最大的计算机网络，它将分布在世界各地的不同类型、不同规模的多个计算机网络通过 TCP/IP 协议连接起来，以实现数据传输和资源共享。Internet 是一个世界范围的信息资源库。人们可以通过 Internet 阅读信息、查阅资料、网上购物，还可以享受远程医疗和远程教学。Internet 上丰富的资源和获取资源的信息交流手段，为人们的工作、学习和生活带来了极大的便利。

Internet 可以说是网络的网络，是一个最大的广域网。Internet 最初起源于美国国防部高级研究项目署(ARPA)在1969年建立的一个实验性网络 ARPAnet。该网络将美国许多大学和研究机构中从事国防研究项目的计算机连接在一起，采用分组交换技术，使用报文处理机实现网络互联，实现资源共享，并且能够互换信息，进行电子会议等。1980年 ARPAnet 全面推广 TCP/IP 协议，成功用于异构网络，使得网络上的所有计算机能够相互交流信息。1984年，ARPAnet 分解为两个网络：ARPAnet 作为民用科研网，MILnet 作为军用计算机网络。

1986年，美国国家科学基金会(NSF)采用 TCP/IP 通信协议，建立了 NSFnet 广域网，且与 ARPAnet 联通，以便实现资源共享。并且逐步取代了 ARPAnet 网成为 Internet 的主干网。1989年 MILnet 与 NSFnet 实现连接后，开始采用 Internet 这个名称。Internet 的早期结构如图5-1所示。

1989年，由欧洲核子研究中心(CERN)开发成功的万维网(World Wide Web，WWW)为 Internet 实现广域超媒体信息截取/检索奠定了基础。从此，Internet 开始进入迅速发展时期。

自20世纪90年代以来，随着 Internet 服务的增强，人们开始利用其功能进行各种业务，使 Internet 逐步走向民间，走向商业化。

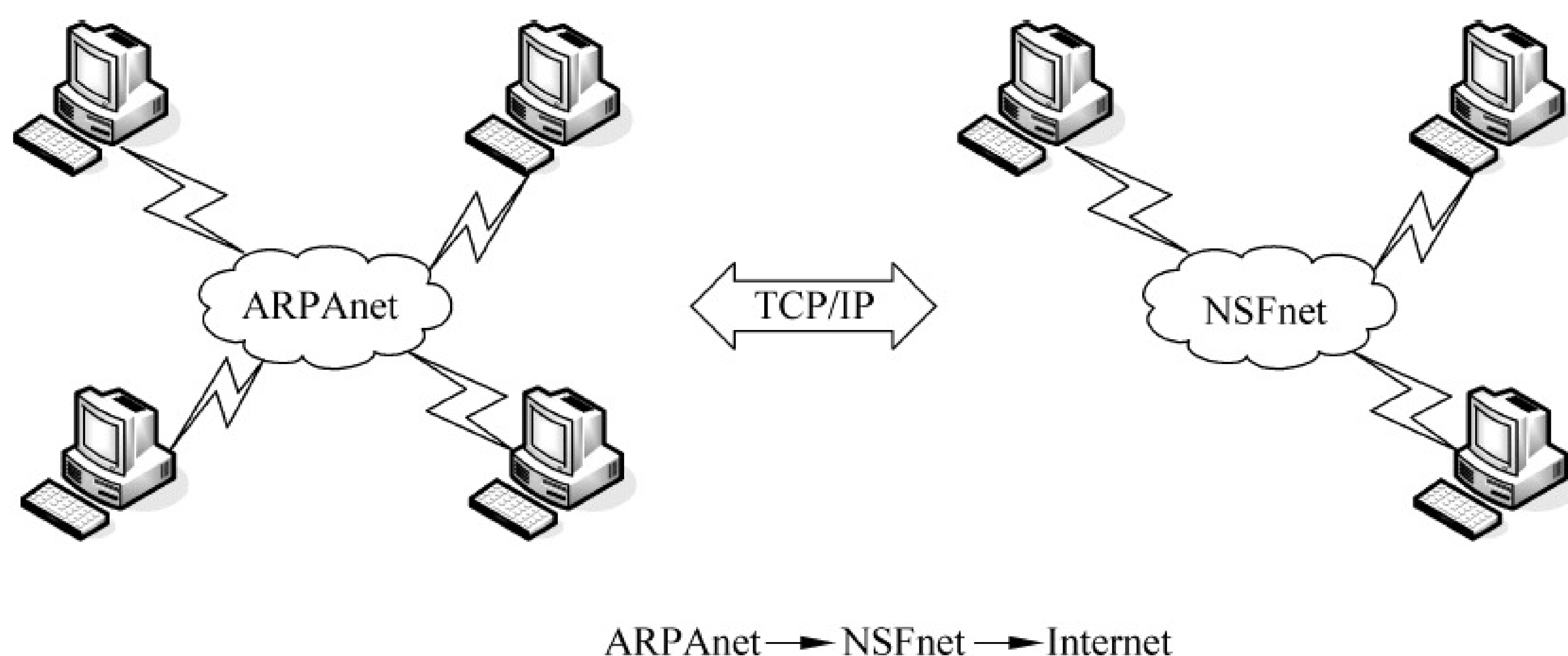


图 5-1　Internet 的早期结构

归纳起来，Internet 的发展可以分为三个阶段：军用实验阶段(1969—1984 年)；学术应用阶段(1984—1992 年)；向商业应用过渡阶段(1992 年后)。

2. Internet 在中国的发展

我国的 Internet 起步较晚，但发展迅速。1986 年，中国科学院通过长途拨号方式进行国际联机数据库检索，拉开了我国 Internet 发展的帷幕。从 1994 年 4 月正式加入 Internet，到 1996 年，我国的 Internet 形成了中国科技网 CSTNET、中国教育和科研计算机网 CERNEET、中国公用计算机互联网 CHINANET 和金桥信息网 CHINAGBN 四大主流体系。

Internet 在中国的发展主要经历了起步和发展两个阶段。

1986—1994 年为起步阶段，以拨号上网为主，主要使用电子邮件服务，这个阶段是以中国科学院高能物理研究所为代表的。

从 1994 年开始进入发展阶段，实现了与国际 Internet 的 TCP/IP 连接，从而开始了 Internet 全功能服务，全国范围的计算机网络相继建立。

到 2008 年 6 月，经国务院批准，我国全国性的骨干互联网有 8 个。下面简单介绍国内的几个主要互联网。

中国公用计算机互联网(ChinaNet)：由中国电信负责建设与经营管理，俗称 163。ChinaNet 的主页地址是 http://www.bta.net.cn，国际线路的容量为 230 225MB。

宽带中国 CHINA169 网：由中国网通集团公司经营，俗称 169。国际线路的容量为 211 137(含有 CNCNet 网)MB。

中国联通公用计算机互联网(UNINet)：由中国联合通信有限公司负责建设与经营管理。UNINet 的主页地址是 http://sms.cnuninet.com，国际线路的容量为 4 319MB。

中国网通公用互联网(CNCNet)：由中国网络通信有限责任公司负责建设与经营管理。CNCNet 的主页地址是 http://www.cnc.net.cn。

中国移动互联网(CMNet)：由中国移动通信集团公司负责建设与经营管理。CMNet 的主页地址是：http://www.chinamobile.com，国际线路的容量为 27 860MB。

中国教育科研网(CERNet)：中国教育科研网由国家投资建设，教育部负责管理。

CERNet 的主页地址为 http://www.cernet.edu.cn,国际线路的容量为9932MB。

中国科技网(CSTNet):中国科技网由国家投资和世界银行贷款建设,由中国科学院网络运行中心负责运行管理。CSTNet 的主页地址为 http://www.cnc.ac.cn,国际线路的容量为9010MB。

中国国际经济贸易互联网(CIETNet):面向全国外经贸系统事业单位的专用互联网。由外贸经济合作部下属的中国国际电子商务中心负责建设和管理。CIETNET 的网址是 http://www.ciet.net,国际线路的容量为2MB。

3. 下一代 Internet(Internet Ⅱ)

Internet 的产生和发展已对世界经济产生了巨大的影响,然而,随着网络规模的持续膨胀和新型网络应用需求的不断增长,现有的 Internet 面临着许多挑战。一方面,现有的 Internet 可扩展性差,IP 地址空间不够,将来会需要大量的公有地址(比如信息家电、移动终端、工业传感器、自动售货机、汽车等对地址的需求),IPv4 无法为急剧增长的用户群提供服务;另一方面,新的分布式多媒体在线应用(比如对服务质量和安全高度敏感的端到端实时语音及视频应用),对 Internet 的影响以及引出的问题已超出了目前 IPv4 所能解决的范围。这就需要一个新的网络体系结构,提供更高更完善的网络性能,包括更高的带宽、更高的服务质量(QoS)、可移动性和网络安全性、智能化的网络管理模式等。另外,无处不在的信息与通信服务方式,都需要通过探索新的技术来解决这些问题。在这样的背景下,下一代 Internet(Internet Ⅱ)应运而生。下一代 Internet 由大学高级 Internet 发展联盟(U-CAID)于1998年提出,有170所大学参加,致力于发展 IPv6、多终点传输、服务质量技术、数字图书馆及虚拟实验室等应用。其中 IPv6 通过采用128位的地址空间替代 IPv4 的32位地址空间来扩充 Internet 的地址容量,使得 IP 地址在可以预见的时期内不再成为限制网络规模的因素,同时在安全性、服务质量及移动性等方面有了较大的改进。IPv6 解决的不仅仅是 IP 地址空间的问题,更重要的是推动业务创新,使 Internet 能够承担更多的任务,为以 IP 为基础的网络融合,奠定了坚实的基础。

以 IPv6 为基础核心协议的下一代网络,将成为国家信息化的基础设施,并带动国民经济,从基础教育、科研、医疗、能源、交通、金融、环保、工业到家电产业等各行各业的全面发展。在人类社会与人类生活的方方面面,无处不在的网络将提供无处不在的信息与通信服务。

4. Internet 的基本组成

(1) 物理网络

Internet 最基本的部件是物理网络,Internet 上的所有计算机是通过成千上万根电缆、光缆或无线通信设备以及连接器组成的一个有机的物理网络;物理网络是传播信息的真实载体。

(2) 通信协议

在 Internet 上传送的每个消息至少通过三层协议:网络协议(Network Protocol),它负责将消息从一个地方传送到另一个地方;传输协议(Transport Protocol),它管理被传送内容的完整性;应用程序协议(Application Protocol),作为对通过网络应用程序发出的一个请求的应答,它将数据转换成人类能识别的形式。

(3) 网络工具

6 大基本工具：远程登录、文件传输、网络漫游和资源挖掘工具、电子邮件工具、网络聊天工具以及流媒体播放工具。

5. Internet 的未来发展方向

(1) 未来 Internet 的用户需求将向 WWW、移动性和多媒体方向发展。

(2) 未来 Internet 的应用将包括与广播媒体、通信业务以及出版媒体的综合。

(3) Internet 社会就是信息社会。信息社会将具有 5 大特征：技术的多样性、业务的综合性、行业的融合性、市场的竞争性和用户的选择性。

(4) 未来 Internet 将给任何人(anybody)、在任何时间(anytime)、任何地点(anywhere)、以任何接入方式(any connection)和可承受的价格，提供任何信息(any information)并完成任何业务(any service)。

5.1.2 精彩纷呈的万维网

1. WWW 基本概念

WWW 又称为万维网，简称为 Web，中文名称为万维网。WWW 不是普通意义上的物理网络，它是建立在 Internet 上的一种多媒体集合，它通过超文本(Hypertext)的表达方式，利用超链接(Hyperlink)将 WWW 上的数字信息连接在一起。

Web 服务采用基于客户机/服务器的工作模式。整个 Web 服务系统包括客户机端、服务器端和超文本传输协议 HTTP 三个部分。

客户机端计算机上运行着 WWW 客户程序，如 IE 浏览器。Web 客户机端程序为使用 Web 服务的用户提供一个良好的界面，使用户能够方便地使用 Web 服务，同时负责将用户所发出的 Web 服务请求发送到服务器端。

WWW 服务器也称为 Web 服务器，把信息组织为分布的超文本，信息资源以 Web 页的形式存储在 Web 服务器中。Web 服务器上运行着服务器端应用程序，随时处理来自客户机端的 Web 服务请求，在执行了服务请求后，将处理的结果返回给客户端的计算机，以用户需要的形式显示在客户机端的计算机上。

Web 服务的实现是建立在超文本传输协议 HTTP 上的，HTTP 是 Internet 网上的应用层协议，是 Web 服务器和 Web 浏览器之间的通信语言，所有的 Web 服务器和 Web 浏览器必须遵循该协议，才能发送或接收超文本文件。

为了实现服务器端与客户机端用户信息的传输，HTTP 定义了 Web 通信的 4 个步骤：

(1) 服务器与客户机建立连接。

(2) 客户机端向服务器端递交请求，在请求中指明所要求的特定文件。

(3) 如果请求被接受，则服务器发回一个应答，在应答中至少包含状态编号和该文件内容。

(4) 客户机与服务器断开连接。

2. WWW 的核心技术

网页与主页：网页是网站所提供的 Web 服务的基本信息单位，也称 Web 页，是由一个 HTML 文件以及相关的图形图像、声音、动画等元素组成。一个网站包含若干个网

页,网页上包含超链接,通过超链接连到其他网页或网站。使用者访问某个网站时的起始页叫做主页。

超链接:WWW 服务器通过超链接将单词、词组、符号、图像多种信息单元作为连接点,将信息相互连接在一起,这些连接点是当前网页与其他网页或网站之间的连接点。使用者可以通过超链接,从当前位置跳转到链接指定的位置,从而方便获取自己所需的信息。

超文本:WWW 中 Web 页采用超级文本(Hyper Text)的格式,即可以含有指向其他 Web 页或其本身内部特定位置的超级链接,或简称链接。可以将链接理解为指向其他 Web 页的“指针”。链接使得 Web 页交织为网状。

超媒体:一种将文本、图像、图片、声音、动画和视频等集成于一体的媒体技术,它将文本、图像、图片、声音和动画等集成为一个相关的信息系统,通过超链接将它们相互链接起来。

超文本标记语言(HTML):HTML 是 Hypertext Markup Language(超文本标记语言)的简称,它是 Web 页的标记语言,用来描述 Web 页的逻辑结构和属性。当用户从 Web 服务器取到一个文件后,用户需要在自己的屏幕上将它正确无误地显示出来。由于将文件放入 Web 服务器的人并不知道将来阅读这个文件的人到底会使用哪一种类型的计算机或终端,要保证每个人在各自的屏幕上都能读到正确显示的文件,必须以某种各类型的计算机或终端都能“看懂”的方式来描述文件,于是就产生了 HTML——超文本标记语言。HTML 文档本身是文本格式的,用任何一种文本编辑器都可以对它进行编辑。HTML 有一套相当复杂的语法,专门提供给专业人员用来创建 Web 文档,一般用户并不需要掌握它。在 UNIX 系统中,HTML 文档的后缀为“.html”,而在 DOS/Windows 系统中则为“.htm”或者“.html”。图 5-2 是 Web 服务的访问过程。

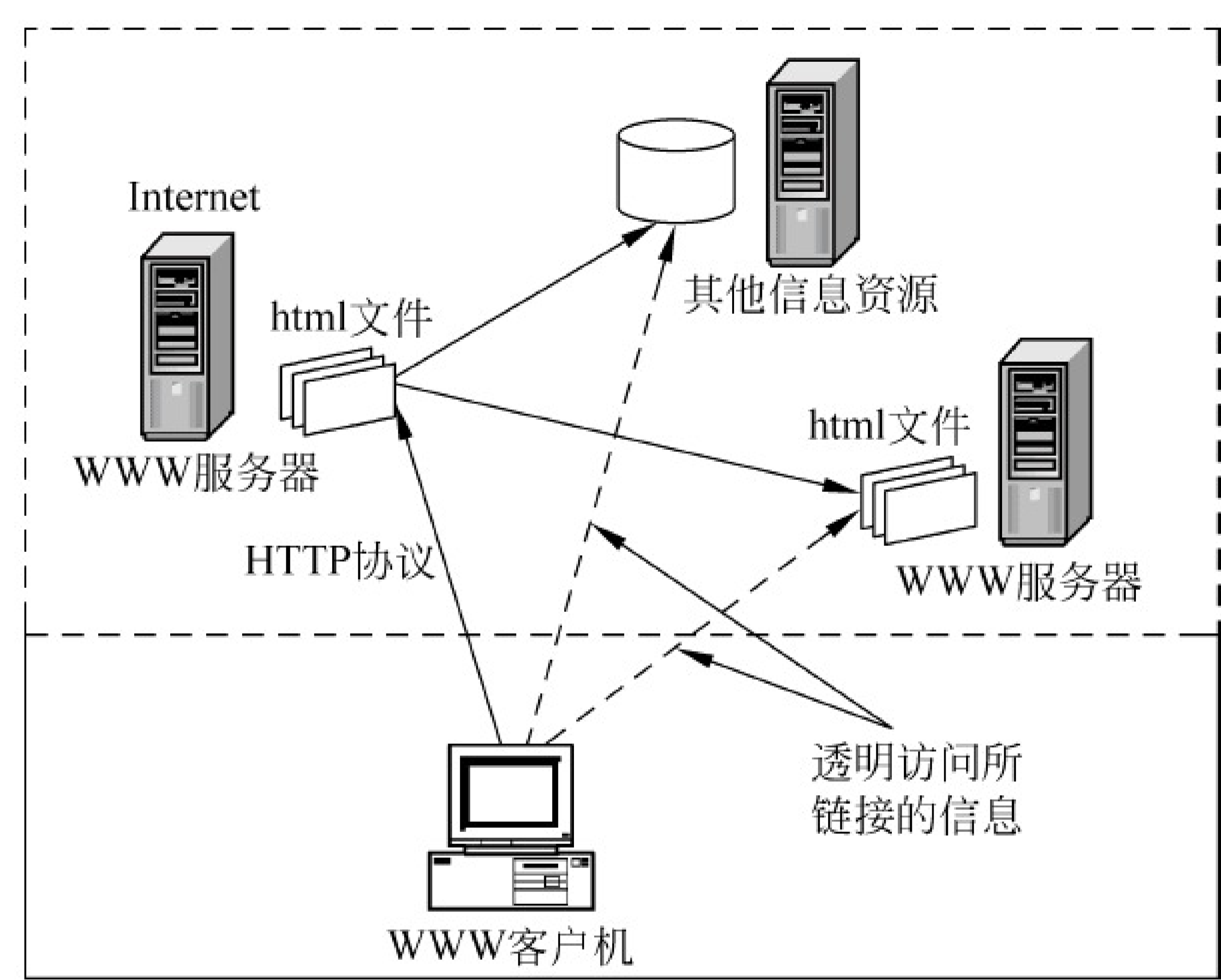


图 5-2　Web 服务的访问过程

3. URL 与信息定位

“统一资源定位符 URL”给互联网上的资源的位置提供了一种抽象的识别方法,并用这种方法给资源定位。只要能够对资源定位,系统就可以对资源进行各种操作,如存取、

更新、替换和查找其属性等。上述的“资源”是指在因特网上可以被访问的任何对象,包括文件目录、文件、文档、图像、声音等以及与因特网相连的任何形式的数据。“资源”还包括电子邮件的地址和新闻讨论组(Uses Network)Usenet,或 Usenet 新闻组中的报文。

URL 由三部分组成:被访问的信息的类型、信息所在服务器的位置以及信息在服务器的位置。URL 的通用格式是:

```
协议名://服务器名[:端口号]/路径/文件名
```

例如:

```
http://www.tsinghua.edu.cn/                  ;通过 HTTP 查看网页
ftp://210.45.176.68/pub/dos/readme.txt       ;通过 FTP 下载名为 readme.txt 的文本文件
rtsp://210.45.176.10/movies6/毕业生.rm       ;在所连接的主机上在线观看视频节目
mms://210.45.176.38/cctv1                    ;在所连接的主机上在线观看电视节目
```

5.1.3 IP 地址与域名

在 Internet 上进行信息交换的基本条件,就是在网络上的主机必须有一个不与其他计算机重复的地址。主机(Host)指的是每台与 Internet 连接的计算机或设备。

Internet 的地址分为两种形式:即用数字表示的 IP 地址和用字母表示的域名地址。

1. IP 地址

基于 IP 协议的因特网,目前已经发展成为当今世界上规模最大、拥有用户最多、资源最广泛的通信网络。IP 协议也因此成为事实上的业界标准,以 IP 协议为基础的网络已经成为通信网络的主流。IP 协议的重要功能就是屏蔽主机原来的物理地址,从而在全网中使用统一的 IP 地址。

IP 地址是用来标识网络中的一个通信实体,比如一台主机,或者是路由器的某一个端口。而在基于 IP 协议的网络中传输的数据包,也都必须使用 IP 地址来进行标识。每个被传输的数据包要包括源 IP 地址和目的 IP 地址。当数据包在网络中进行传输时,这两个地址要保持不变,以确保网络设备总能根据确定的 IP 地址,将数据包从源通信实体送往指定的目的通信实体。

一个 IP 地址只能被一个网络设备所使用,但一个网络设备和计算机可以同时使用多个不同的 IP 地址。

在 IPv4 协议中,IP 地址由 4 个字节(32 位二进制数)组成。为方便书写和记忆,通常以点划分的十进制数来表示,称为点分十进制。如:一个 IP 地址点分十进制形式为:202.114.206.202,其对应的二进制数表示方法为:11001010 01110010 11001110 11001010。

IP 地址包含两部分信息:网络地址和主机地址。所以 IP 地址分为网络地址(Netid)部分和主机地址(Hostid)部分。其中 Netid 标识一个网络(表示入网主机所在的网络),而 Hostid 标识在该网络上的一个主机(表示入网主机在本网段中的标识)。寻址时,首先根据 IP 地址中的网络号找到相应网络,再按主机号找到具体的主机。实际上,IP 地址是一种在网络层用来标识主机的逻辑地址。当数据包在物理层传输时,由 ARP 提供的地址映射服务,把 IP 地址转换成物理地址。

2. IP 地址分类

人们按照网络规模的大小，通常将因特网 IP 地址分成 5 种类型：A 类、B 类、C 类、D 类、E 类。其中 A、B 和 C 三类地址被称为基本的 Internet 地址，供用户使用，为主类地址（如图 5-3 所示）。D 类和 E 类地址为次类地址，D 类地址被称为组播地址，E 类地址是为试验性用途而保留的。

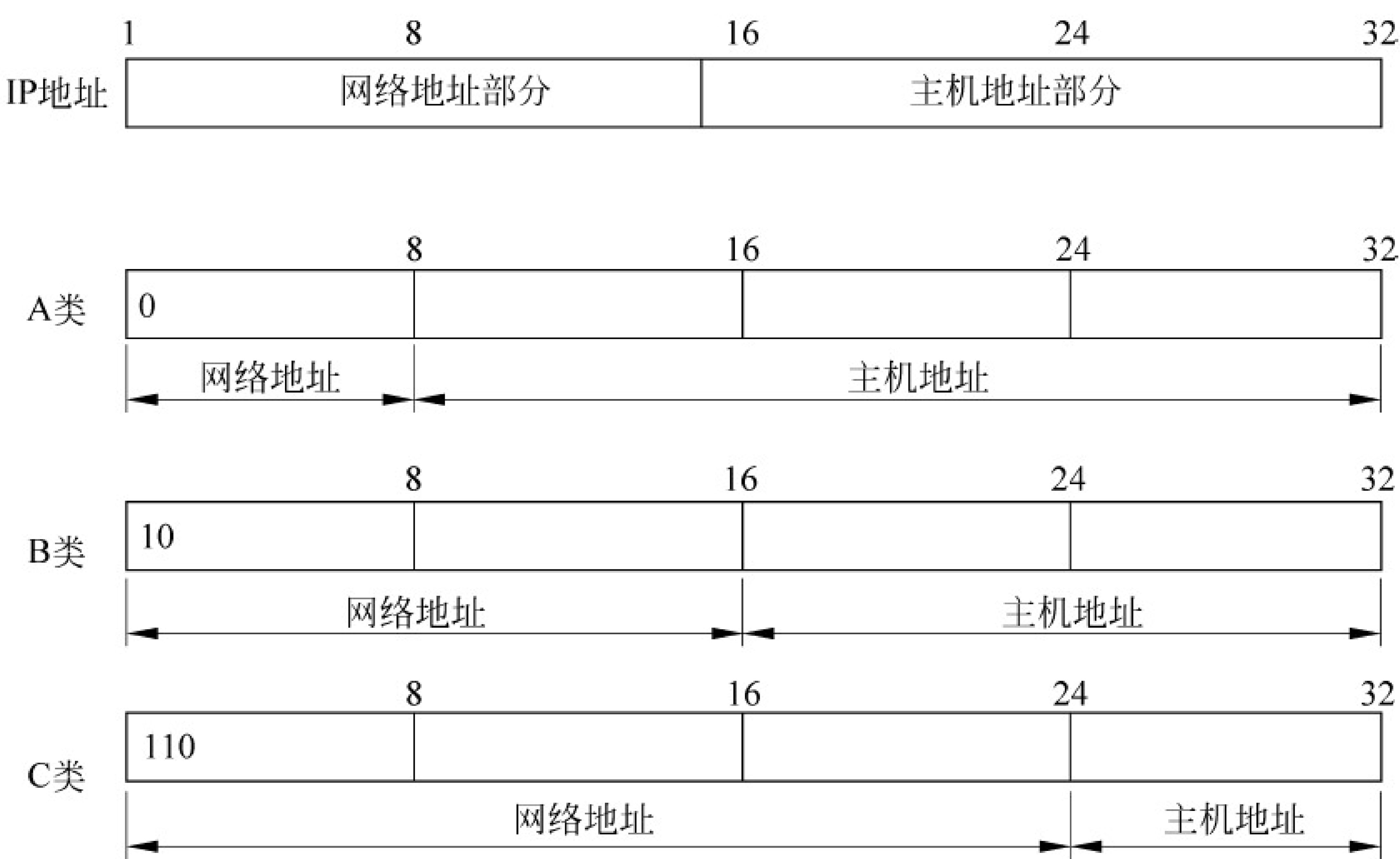


图 5-3　IP 地址分类图

（1）A 类地址

A 类地址的网络标识占 1 个字节，第 1 位为“0”，其余 7 位为网络号。后 3 个字节为主机号。因为网络地址部分全“0”或全“1”不能表示具体的网络地址，而主机地址部分全“0”或全“1”，也不能表示具体的主机地址，所以 A 类地址中网络数有 2^7-2 个，每个网络包含 $2^{24}-2$ 台主机。A 类网络能够容纳的主机数目是最多的，而其网络数量有限，通常分配给拥有大量主机的网络，如一些大公司（如 IBM 公司等）和因特网主干网络。

（2）B 类地址

B 类地址的网络标识占 2 个字节，第一个字节的前两位为“10”，允许有 $2^{14}-2$ 个网络，每个网络大约允许有 $2^{16}-2$ 台主机。主要用于一些国际大公司和政府机构等构成中等规模的网络。

（3）C 类地址

C 类地址的网络标识占 3 个字节，第一个字节的前三位为“110”，允许有 $2^{21}-2$ 个网络，每个网络允许有 254 台主机。通常分配给节点比较少的网络，主要用于一些小公司和研究机构等小型网络。

（4）D 类地址

D 类地址的第一个字节的前 4 位为“1110”，通常用于已知的多点传送或者组播的寻址，主要是留给 Internet 体系结构委员会 IAB 使用。

(5) E类地址

E类地址的第一个字节的前5位为“11110”。是一个实验性地址,保留给将来使用。

IP地址不是任意分配的,必须由国际组织统一分配。分配A类IP地址的国际组织是国际网络信息中心NIC;分配B类IP地址的国际组织是InterNIC、APNIC、ENIC;分配C类IP地址的组织是国家或地区网络的NIC。

3. 专用IP地址及特殊IP地址

(1) 专用IP地址

为了支持局域网发展和联网,RFC 1918定义了专用IP地址。由于大多数因特网路由器不转发携带本地IP地址的分组,本地主机必须通过网络地址迁移服务器(NAT或代理服务器)才能访问因特网。因特网工程任务组IETF规定了下列IP地址供单位内部网使用,可以避免与合法的Internet地址发生冲突。

- 10.0.0.0～10.255.255.255,1个A类地址;
- 172.16.0.0～172.31.255.255,16个连续的B类地址;
- 192.168.0.0～192.168.255.255,256个连续的C类地址。

企业内部网的主机的IP地址设置成专用IP地址,进行企业内部的网络应用;并可通过代理服务器访问因特网(如图5-4所示)。这样只需要申请少量的因特网IP地址,既解决了地址不足的问题,又解决了网络安全问题。

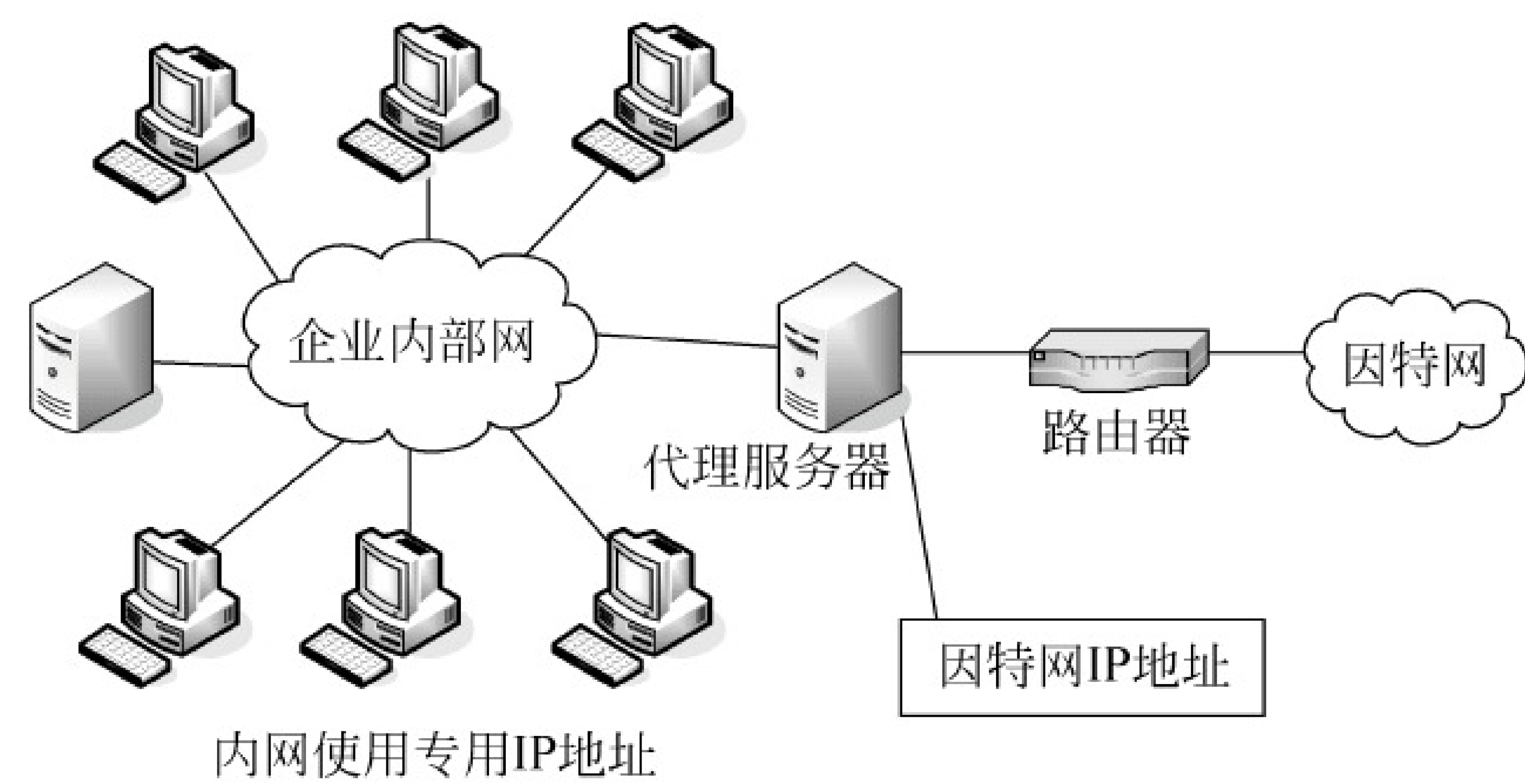


图5-4　企业网通过代理服务器上网

(2) 特殊IP地址

特殊IP地址列表如表5-1所示。

表5-1　特殊IP地址列表

特殊地址	网络地址	主机地址	源地址或目的地址	实例说明
网络地址	特定	全0	都不是	不分配给任何主机,仅用于表示某个网络的网络地址;例:202.114.206.0
直接广播地址	特定	全1	目的地址	不分配给任何主机,用作广播地址,对应分组传递给该网络中的所有节点(能否执行广播,则依赖于支撑的物理网络是否具有广播的功能);例:202.114.206.255

续表

特殊地址	网络地址	主机地址	源地址或目的地址	实例说明
受限广播地址	全 1	全 1	目的地址	称为有限广播地址，通常由无盘工作站启动时使用，希望从网络 IP 地址服务器处获得一个 IP 地址；例：255.255.255.255
本网络的本主机	全 0	全 0	源地址	表示本机地址，仅在系统启动时允许使用，并且永远不是一个有效的目的地址；例：0.0.0.0
本网络的特定主机	全 0	特定	目的地址	本网络的特定主机；例：0.0.0.126
回送地址	127	任意	目的地址	常用于本机上软件测试和本机上网络应用程序之间的通信地址；例：127.0.0.1

4. IP 地址类的确定

如果地址是二进制形式表示的，判断是哪类网络的方法如下：若第一位为 0，则地址为 A 类地址；若前两位为“10”，则地址为 B 类地址；若前三位为“110”，则地址为 C 类地址；若前 4 位为“1110”，则地址为 D 类地址；若前 4 位都是 1，则地址为 E 类地址。

如果地址是点分十进制表示，根据 IP 地址的第一个十进制数判断所属类别，如图 5-5 所示。

	从	到
A类	0.0.0.0	127.255.255.255
B类	128.0.0.0	191.255.255.255
C类	192.0.0.0	223.255.255.255
D类	224.0.0.0	239.255.255.255
E类	240.0.0.0	255.255.255.255

图 5-5　IP 地址范围

5. 子网掩码及其应用

(1) 子网

子网划分是指出于对管理、性能和安全方面的考虑，把单一的逻辑网络划分为多个物理网络，并使用路由器将它们连接起来，这些物理网络统称为子网。

划分子网的方法：将主机地址部分划出一定的位数作为子网标识，其余部分作为主机标识部分。这样 IP 地址就由三部分组成，即网络号、子网号和主机号。其中，网络号确定一个网段，子网号确定一个物理子网，主机号确定子网中的主机。

(2) 子网掩码

要区分 IP 地址中的网络地址与主机地址，需要子网掩码。子网掩码也是一个 32 位地址，其作用是：用于屏蔽 IP 地址的一部分以区分网络标识和主机标识，另外，用于将网络分割成多个子网。只有同在一个子网中的主机才能互相通信联系，否则就要通过路由器了。通过网络标识来判断是否在同一个子网上。

子网掩码取值对应于 IP 地址中网络地址(网络号、子网号)的所有位设置“1”，对应 IP 地址中的主机地址中的每一位设置为“0”。例如位模式：11111111 11111111 11111111 00000000 中，前 3 个字节全 1，代表对应 IP 地址中最高的 3 个字节为网络地址；后一个字节全 0，代表对应 IP 地址中最后的一个字节为主机地址。这种位模式叫做子网模(subnet mask)或子网掩码。

为了使用的方便，子网掩码也常使用“点分十进制法”来表示，如 A 类地址的子网掩码为 11111111 00000000 00000000 00000000，点分十进制形式为 255.0.0.0。同样 B 类地址的子网掩码为 255.255.0.0，C 类地址的子网掩码为 255.255.255.0。

如何从 IP 地址中区分网络地址部分和主机地址部分呢？例如：IP 地址 141.14.2.21 是表示一个未子网化的 B 类地址，还是子网化的地址呢？

网络划分子网实际上是从原来网络的主机部分借位，将其作为子网的网络部分实际上也是对路由选择位进行了扩展，划分出来的子网由于其子网掩码已经不同了，因此不会再属于同一个网段。如图 5-6 所示。

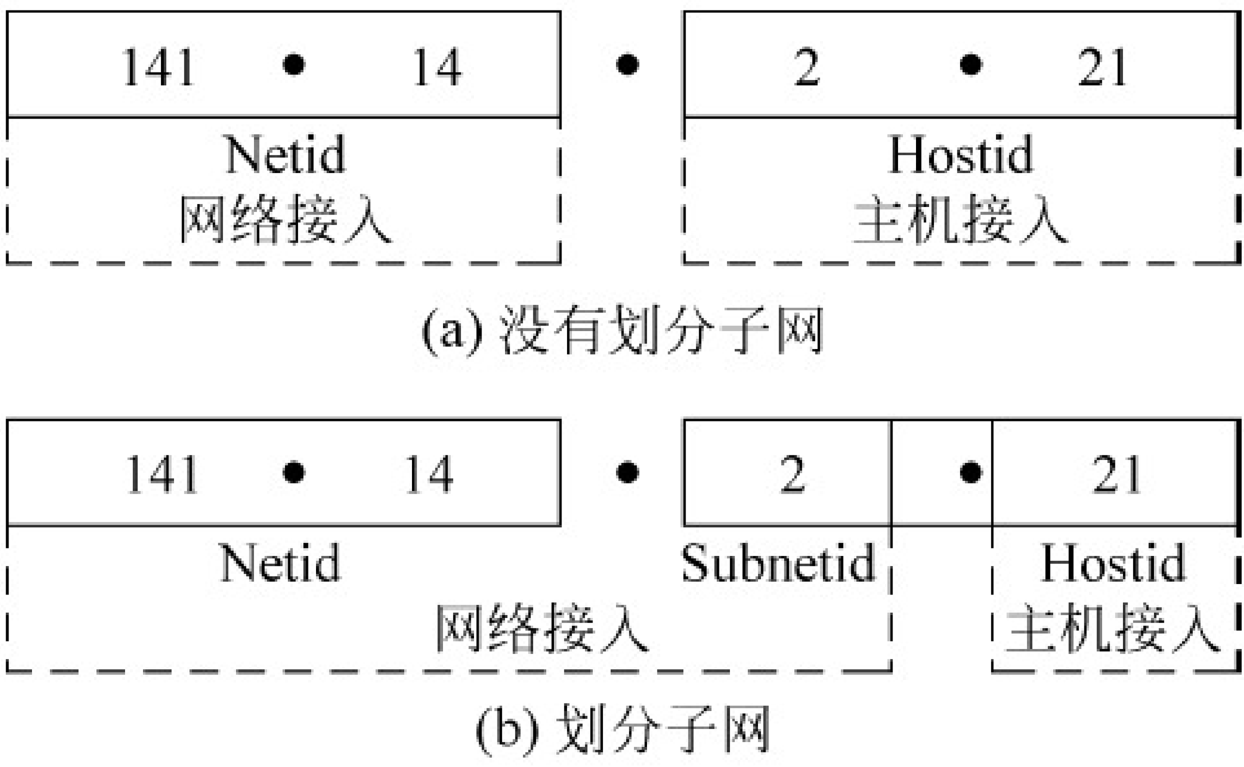


图 5-6 子网划分示意图

IP 地址为 192.9.200.13，其默认的子网掩码为：255.255.255.0。则它的网络号和主机号可按如下方法得到。

将 IP 地址 192.9.200.13 转换为二进制：

11000000 00001001 11001000 00001101

将子网掩码 255.255.255.0 转换为二进制：

11111111 11111111 11111111 00000000

将两个二进制数逻辑与(AND)运算后得出的结果即为网络地址部分。结果转化为点分十进制表示为：192.9.200.0，即网络号为 192.9.200.0。

将子网掩码取反再与 IP 地址逻辑与(AND)后得到的结果即为主机部分。结果为 0.0.0.13，即主机号为 13。

根据以上分析，可以通过下述方式进行子网划分，并确定子网掩码。

① 将要划分的子网数目转换为 2 的 m 次方。如要分 8 个子网，即 $8=2^3$。

② 取上述要划分子网数的 2 的 m 次方的幂。如 2^3，即 $m=3$。

③ 在主机地址部分从高位取 m 位，表示子网地址，剩余主机部分表示子网内主机地址。

如在 C 类网络中，从主机地址部分取 $m=3$ 位表示子网，即 11100000，转换为十进制为 224，子网掩码为 255.255.255.224；如果是 B 类网络，则子网掩码为 255.255.224.0；如果是 A 类网络，则子网掩码为 255.224.0.0。

在这里，子网个数 n 与占用主机地址位数 m 有如下等式成立：$n=2^m$。

根据这些原则，将一个 C 类网络分成 4 个子网。若用的网络号为 192.9.200，则该 C 类网络内的主机 IP 地址就是 192.9.200.1～192.9.200.254(因为全“0”和全“1”的主机地址有特殊含义，不作为有效的 IP 地址)，现将网络划分为 4 个部分，按照以上步骤：$4=2^2$，取 2^2 的幂，即 2，则二进制为 11，占用主机地址的高序位即为 11000000，转换为十进制为 192。这样就可确定该子网掩码为：192.9.200.192，4 个子网的 IP 地址范围分别为：

192.9.200.1～192.9.200.62;
192.9.200.65～192.9.200.126;
192.9.200.129～192.9.200.190;
192.9.200.193～192.9.200.254.

6. 域名系统概述

在 Internet 上访问一台主机，可以使用 IP 地址标识，也可以使用域名标识。人们更愿意使用便于记忆的域名标识符，从而避开难以记忆的 IP 地址，而路由器则只能使用长度固定并有层次结构的 IP 地址。为调解这两种不同的偏好，需要一个把主机名转换成 IP 地址的目录服务。这就是因特网的域名系统(Domain Name System，DNS)的主要任务。域名系统要解决的问题包括：主机名字的管理、主机名字到 IP 地址的映射等。

(1) 域名系统的发展历程

早在 ARPnet 时代，整个网络上只有数百台计算机。因此，只需用一个叫做 hosts 的文件列出所有主机名字与相应的 IP 地址。

1983 年 Internet 开始采用层次结构的命名树作为主机的名字，并使用域名系统 DNS (Domain Name System)。Internet 的域名系统 DNS 被设计成一个联机分布式数据库系统，并采用客户机/服务器模式。因为大多数名字都在本地映射，仅少量映射需要在 Internet 上通信，所以 DNS 系统是高效可靠的。

(2) Internet 的域名结构

Internet 采用层次树状结构(如图 5-7 所示)的命名方法。任何一个连接在 Internet 上的主机或路由器，都有一个唯一的层次结构的名字，即域名。“域”(Domain)是名字空间中一个可被管理的划分。域可以继续被划分为子域，如二级域、三级域等。域名的结构由若干个分量组成，各分量之间用小数点隔开。如：….三级域名.二级域名.顶级域名(stream.cug.edu.cn)。

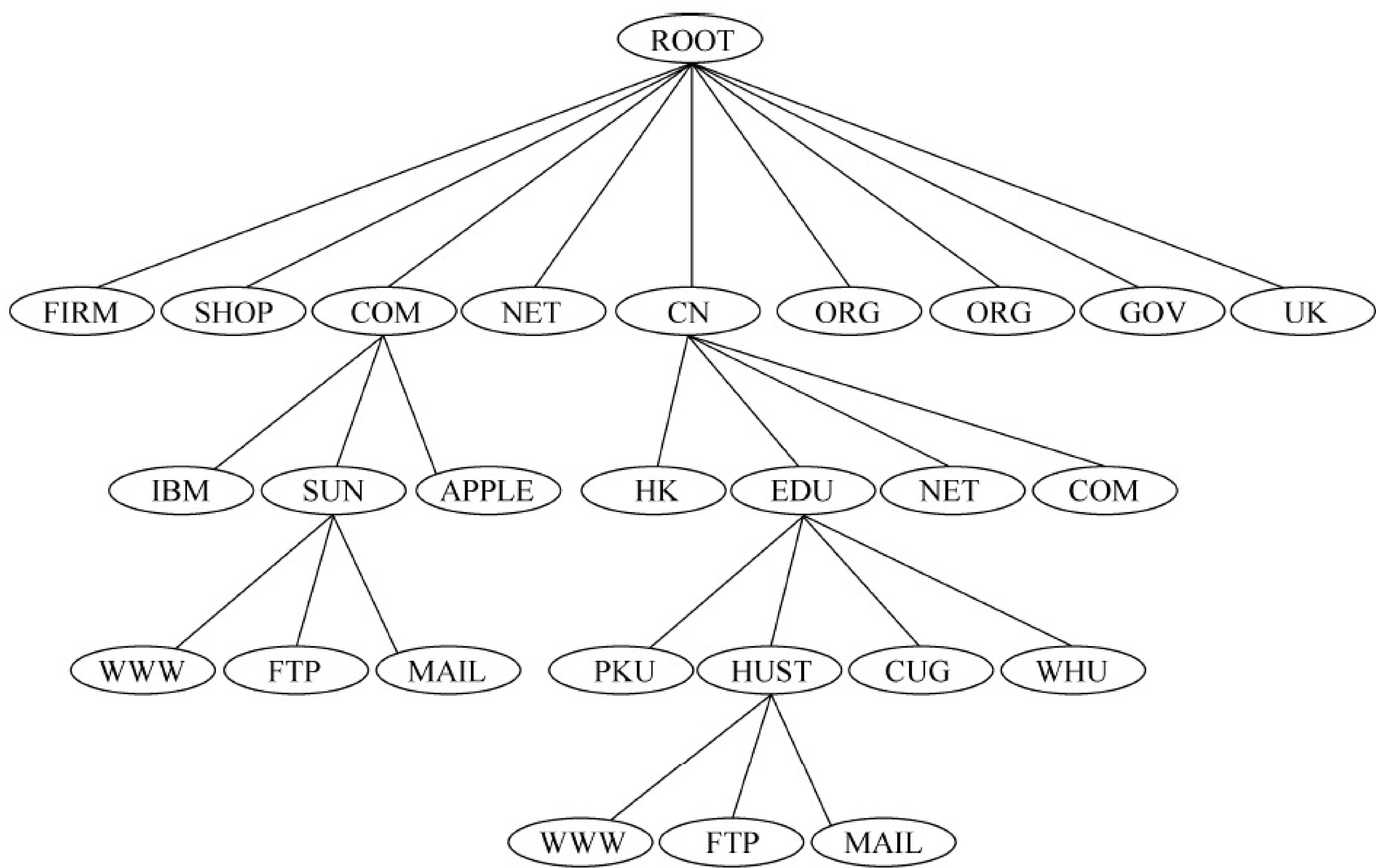


图 5-7 域名结构

每一级的域名都由英文字母和数字组成(不超过63个字符,不区分大小写)。级别最低的域名写在最左边,而级别最高的顶级域名则写在最右边。完整的域名不超过255个字符。

域名只是一个逻辑概念,并不能反映计算机所在的物理地点。

(3) 域名空间的划分

在因特网中,域名空间(树)划分为三个部分:类属域、国家域和反向域。

① 类属域

类属域是指按照主机的类属行为定义注册的主机。类属域有如表5-2所示的字符标号。

表5-2 类属域的标号

标 号	说 明	标 号	说 明
com	商业组织	mil	军事组织
edu	教育机构	net	网络支持中心
gov	政府机构	org	非营利组织
int	国际组织	ac	科研机构

② 国家域

国家域的部分与类属域的格式一样,但使用两个字符的国家缩写,例如,用us代表美国、cn代表中国、uk代表英国、jp代表日本等。二级标号可以是组织的指定,也可以是州、省或区的缩写,例如,hk代表中国香港、hb代表湖北等。

③ 反向域名

反向域名用来将一个IP地址映射为名字。服务器的解析程序向DNS发送一个查询,请求将某个IP地址映射为域名。这种查询叫做反向查询或指针(PRT)查询。反向域用来处理指针查询。反向域的第一级节点叫做arpa,第二级节点叫做in-addr(表示反向地址),域的其余部分定义IP地址。

处理反向域的服务器也是分级的。即表示地址的Netid部分要比Subnetid部分的等级高,而Subnetid部分要比Hostid部分的等级高。读出域的标号时,是从低向高的,如一个IP地址202.114.206.234在反向域中应写为234.206.114.202.in-addr.arpa。

④ 域名解析

域名解析就是将用户提出的名字变换成网络地址的方法和过程,从概念上讲,域名解析是一个自上而下的过程。当DNS客户端提出名字时,接受查询的服务器先从其数据库中寻找,即自己能否解析,若能解析,就将IP地址送回给客户;若不能解析,这个任务就转给下一个DNS服务器,该过程可能进行多次。

例如:客户机向本地服务器发请求,要求解www.baidu.com的IP地址,本地服务器在数据库中寻找相应条目。如果没有,则向根域服务器发出请求,查询代理".com"域的服务器地址。根域收到请求,将代理".com"域的服务器IP地址发给本地服务器。本地服务器收到后向代理".com"域的服务器发送请求,查询"baidu.com"域的服务器的IP地

址。“.com”域服务器将“baidu.com”域服务器IP地址发给本地服务器。本地服务器再向“baidu.com”域服务器请求查询“www”主机的IP地址，“baidu.com”域服务器将“www”主机IP地址发送给本地服务器。最后，本地服务器将最终结果返回客户机，使客户机与www.baidu.com通信。

⑤ 高速缓存

用户有时会连续访问相同的因特网地址，DNS在第一次解析该地址后，将其存放在高速缓存中，当用户再次请求时，DNS可直接从缓存中获得IP地址。充分利用机器的高速缓存，暂存解析后的IP地址，可以提高DNS的查询效率。

⑥ 中国互联网域名管理

1997年，中国互联网网络信息中心（CNNIC）成立，全面负责我国境内的Internet域名注册及IP地址分配管理等工作。CNNIC发布了中国Internet域名体系，最高级为CN。二级域名共40个，设置6个类别域名和34个行政区域名。二级域名中除了EDU的管理和运行由CERNET负责外，其余全部由CNNIC管理。CNNIC的网址为www.cnnic.net.cn，教育网NIC部的网址为www.nic.edu.cn。

任务完成：家庭连接到Internet的方式有多种，以太网＋静态IP地址和ADSL宽带上网是目前普遍的方式。下面分别介绍一下两种上网方式的配置方法。

（1）以太网＋静态IP地址接入方式

右键单击“网上邻居”图标，选择“属性”命令，双击“本地链接1”图标，选择“属性”命令，找到“Internet协议（TCP/IP）”复选项，单击“属性”按钮，在属性对话框中填入通信公司分配给你的网络地址参数。如图5-8所示为校园网分配给用户的地址例子，仅供用户参考。

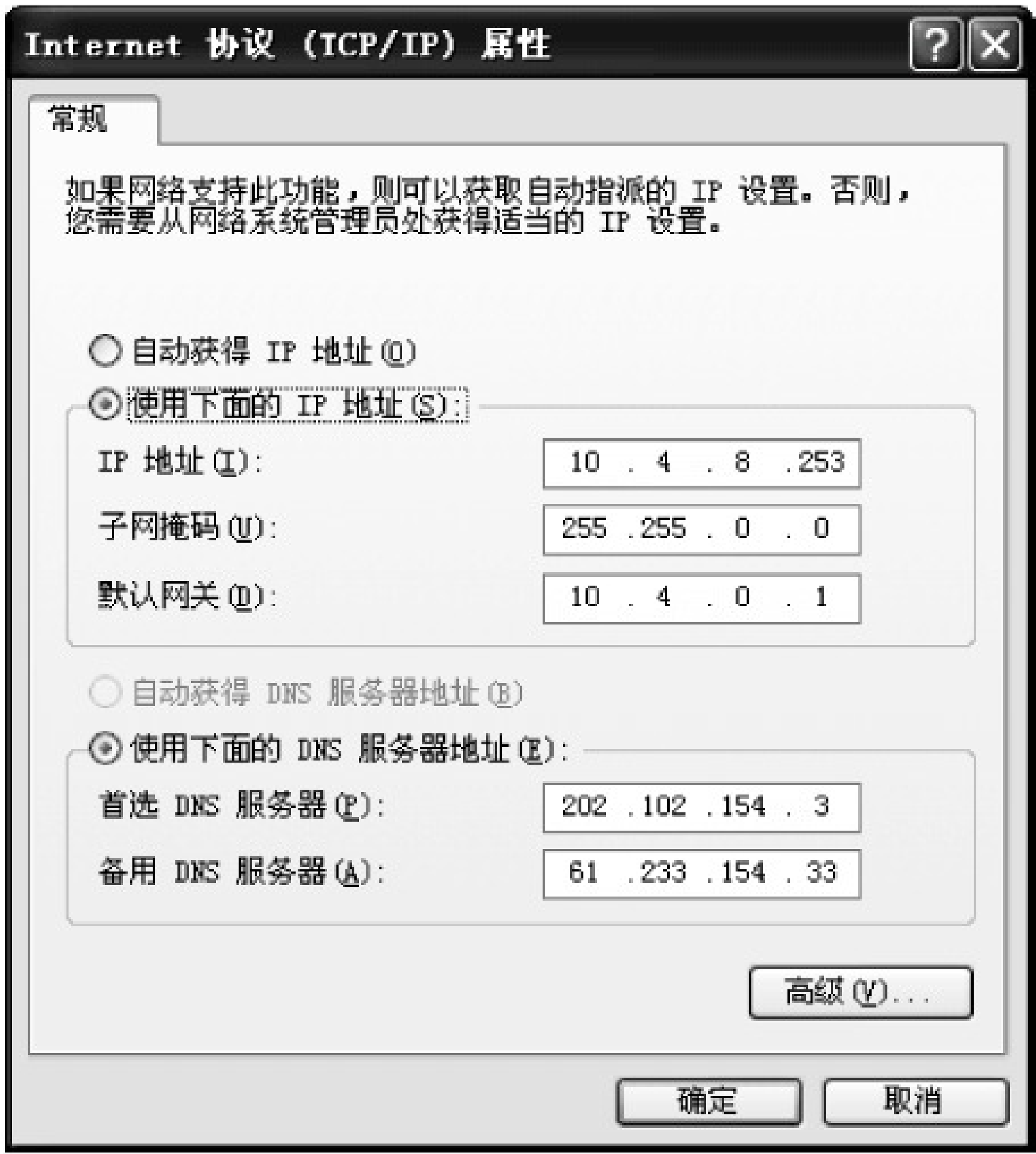


图5-8　“Internet协议（TCP/IP）属性”对话框

（2）非对称数字用户线路（ADSL）参数配置

① ADSL域名服务器（DNS）和IP地址设置

将计算机TCP/IP协议属性里面的DNS和IP地址设成自动获取即可，在上网时系统会采用电信公司的接入服务器自动分配DNS和IP地址。在图5-8中，选择“自动获得IP地址（O）”和“自动获得DNS服务器地址（B）”即可。

② ADSL上网设置步骤（以Windows XP为例）

Windows XP自带了拨号程序所以不用另行安装其他拨号程序，目前ADSL调制解调器绝大部分是外置的，不需要安装驱动程序。直接执行以下操作就可以建立ADSL宽带上网拨号连接。

a）执行“开始”→“所有程序”→“附件”→“通信”→“新建连接向导”命令，弹出“新建连接向导”界面，如图5-9所示。单击“下一步”按钮继续。

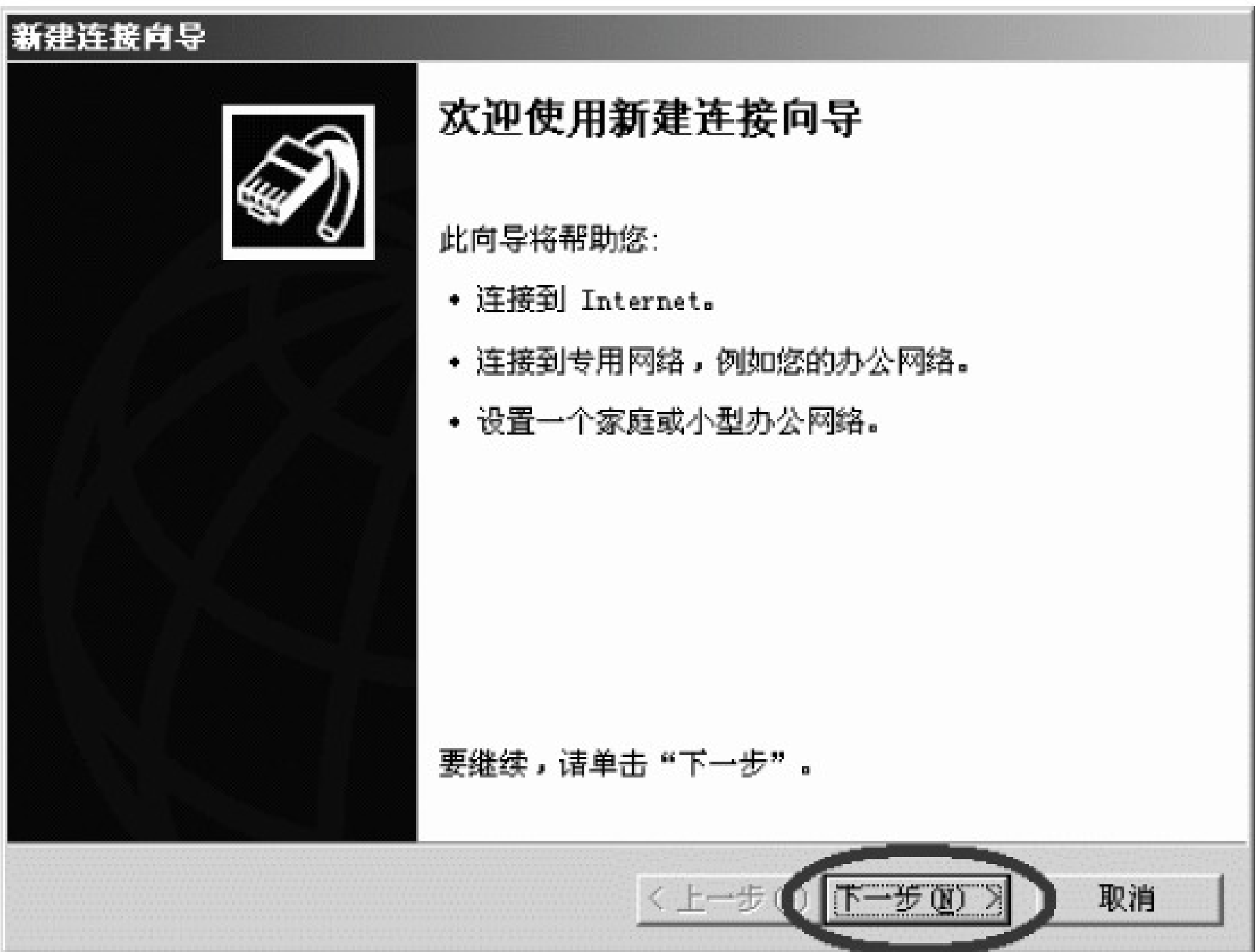


图 5-9　新建连接向导

b）选择“连接到 Internet”选项，然后单击“下一步”按钮，如图 5-10 所示。

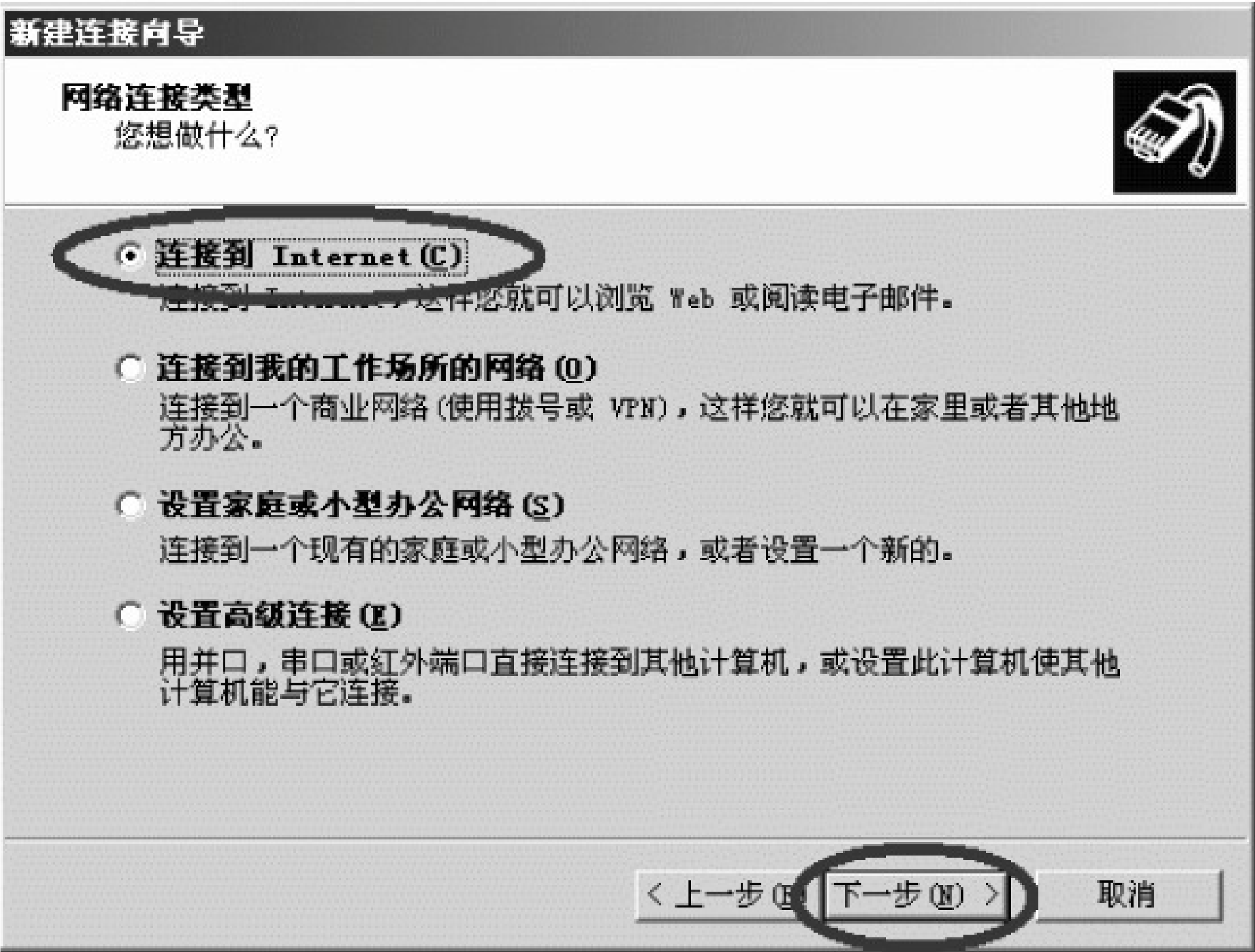


图 5-10　网络连接类型

c）选择“手动设置我的连接”选项，然后单击“下一步”按钮，如图 5-11 所示。

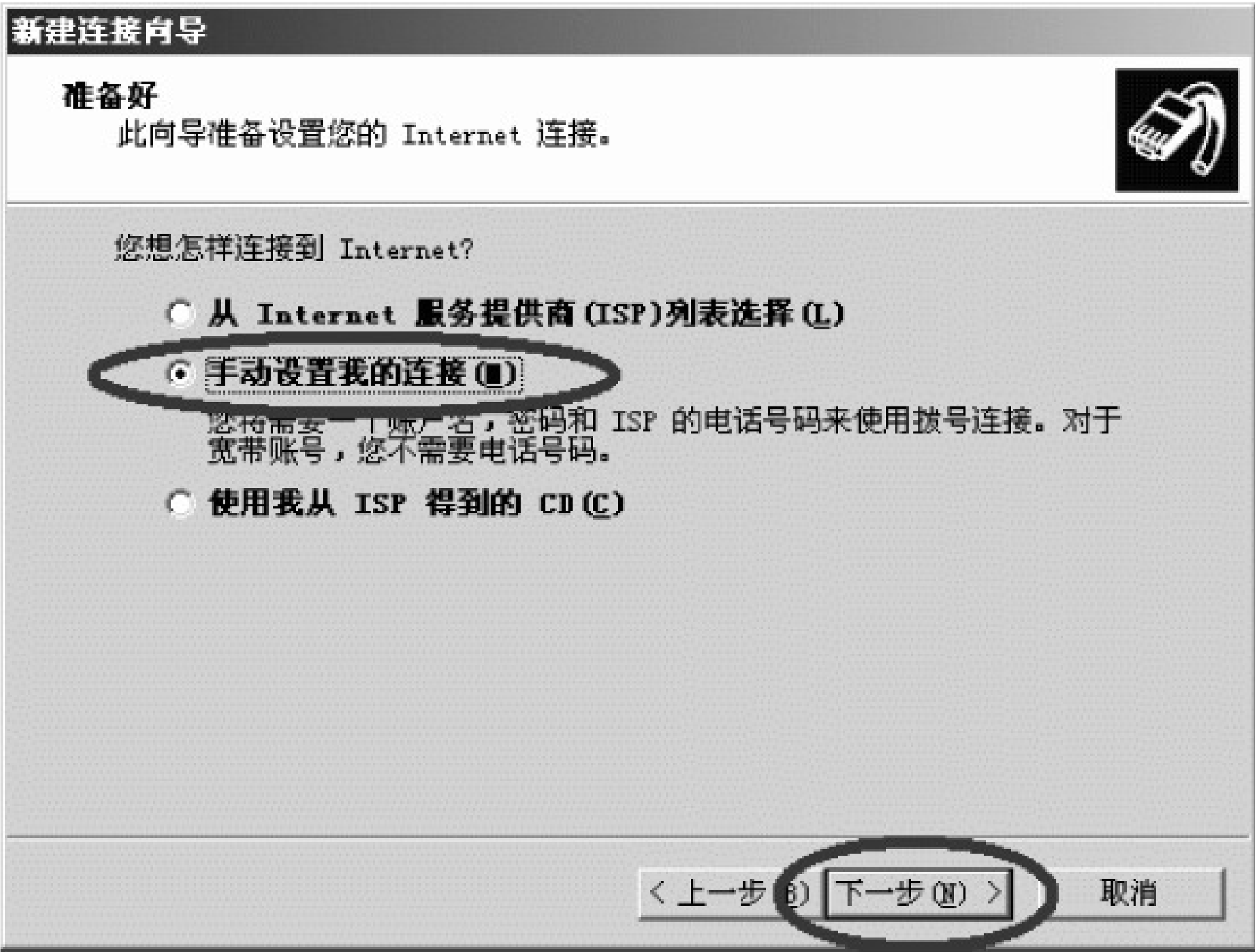


图 5-11　手动设置我的连接

d）选择“用要求用户名和密码的宽带连接来连接”选项，然后单击“下一步”按钮，如图 5-12 所示。

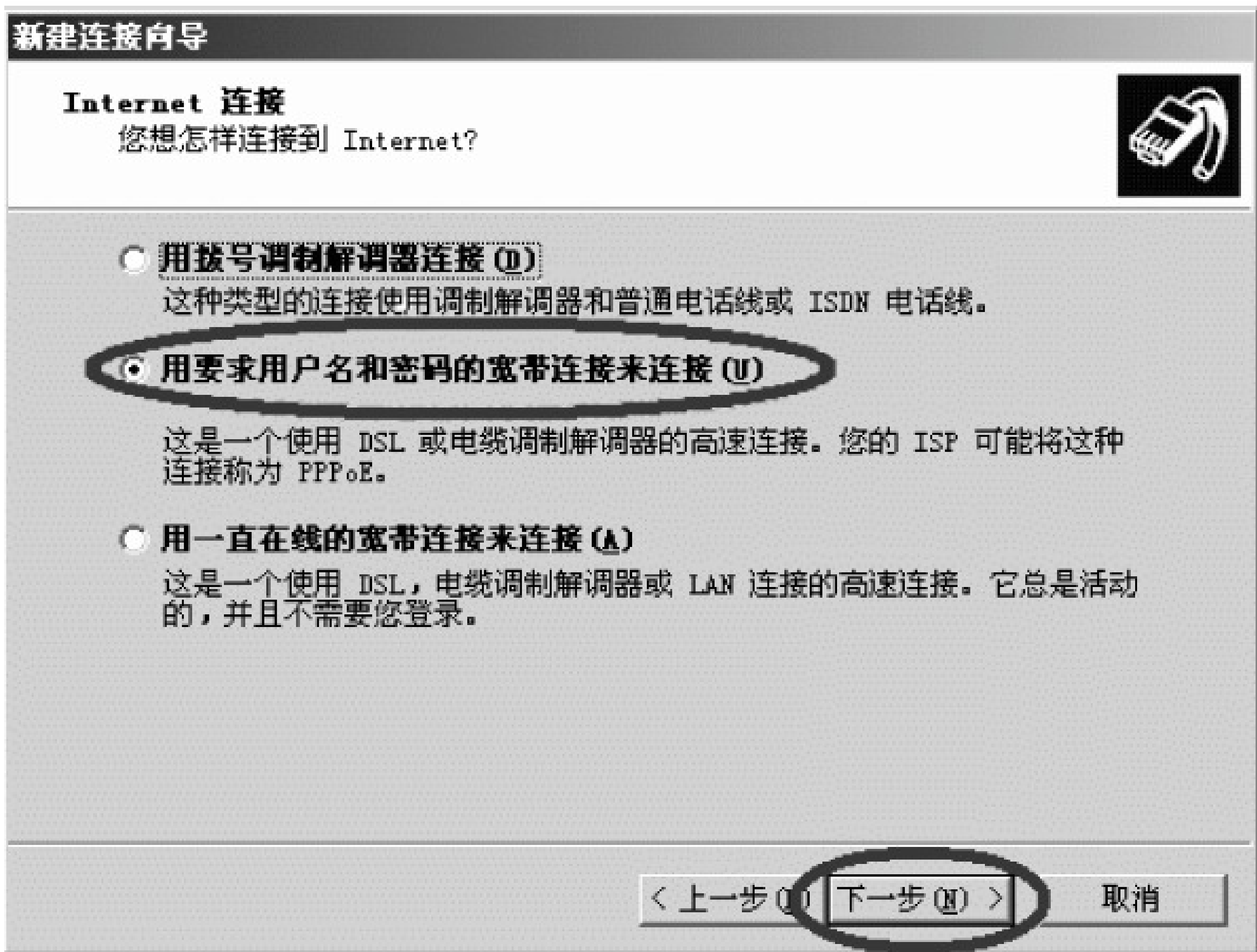


图 5-12　宽带连接

e）在“ISP 名称（A）”栏中输入“ADSL”，如图 5-13 所示。然后单击“下一步”按钮继续。

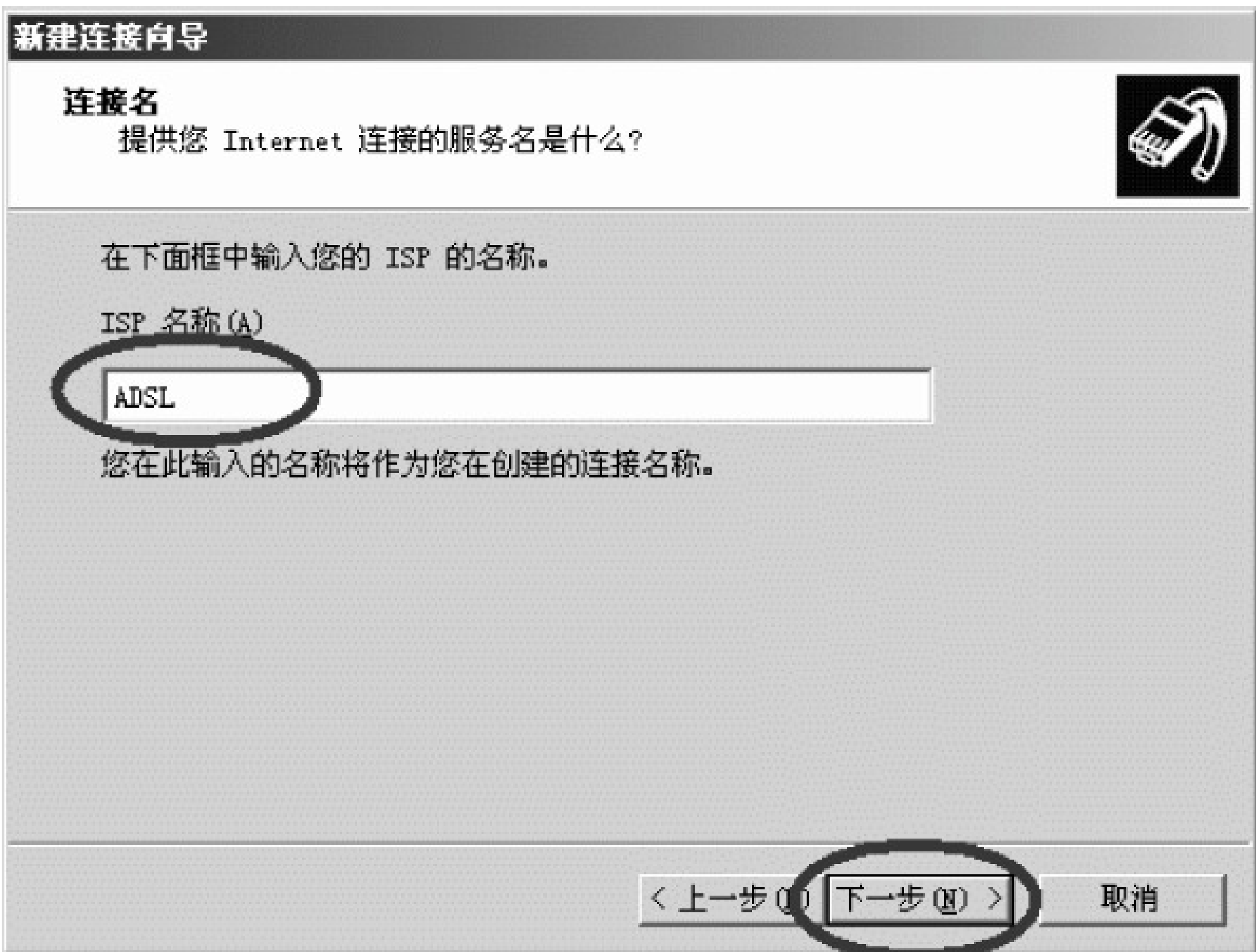


图 5-13　ISP 名称

f）在“用户名”栏中输入用户名，如“xmadsl1”，并输入密码和确认密码，如图 5-14 所示，然后单击“下一步”按钮继续。

g）选中“在我的桌面上添加一个到此连接的快捷方式”复选框，如图 5-15 所示。然后单击“完成”按钮。

h）连接已建立。双击桌面上的拨号快捷方式，拨号连接网络，出现如图 5-16 所示的界面，输入用户名和密码，单击“连接”按钮，登录网络。

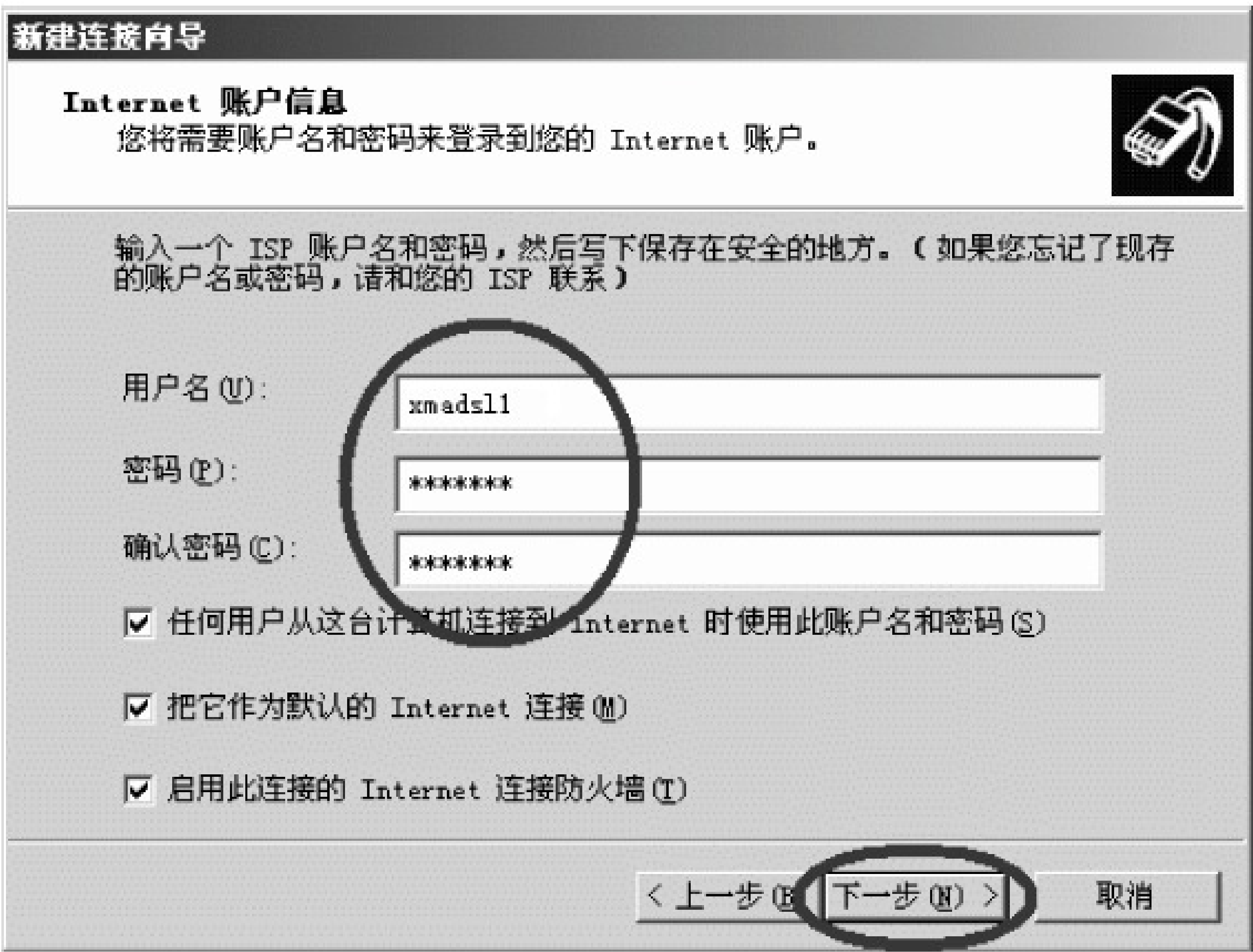


图 5-14　Internet 账户信息

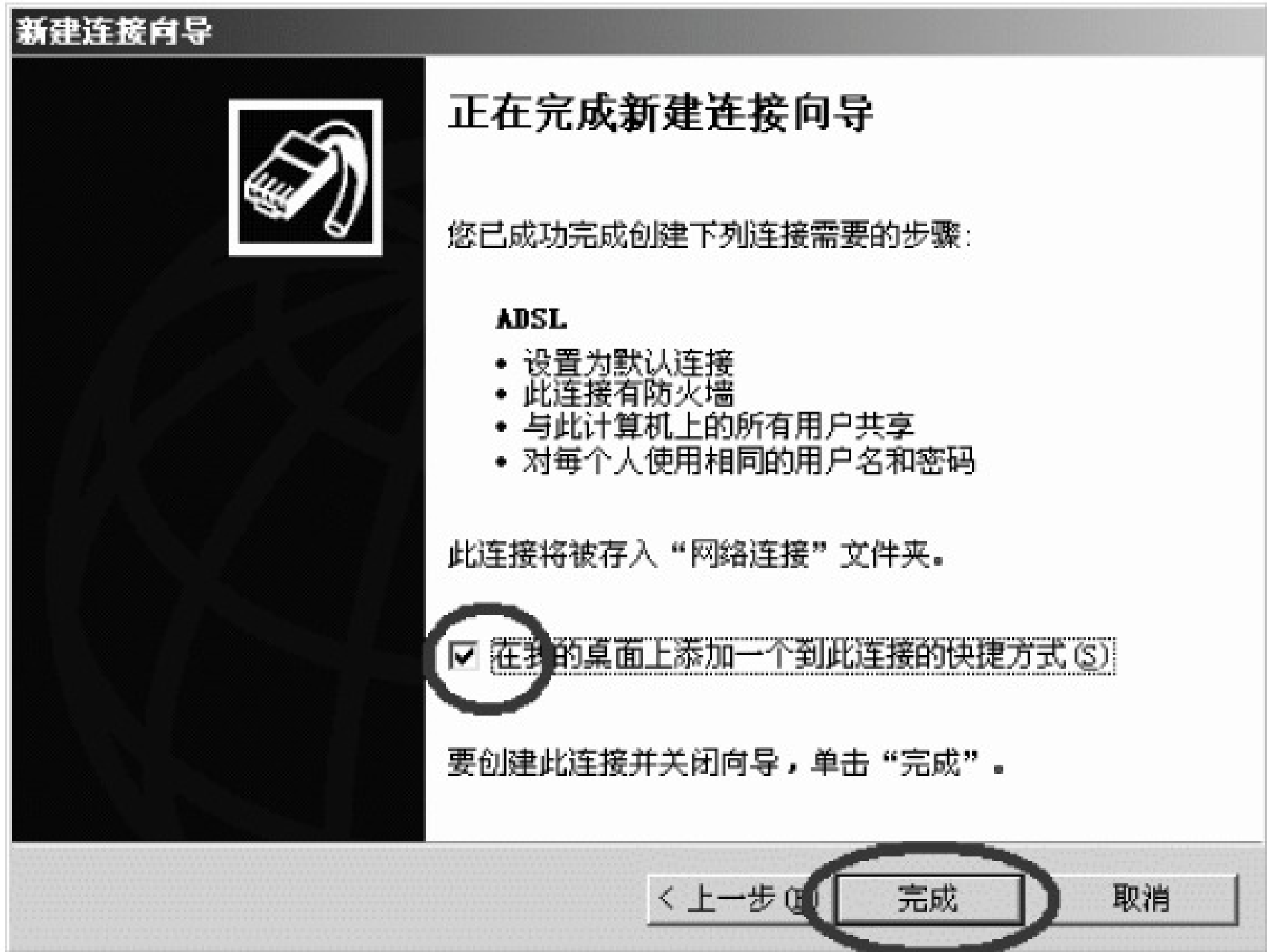


图 5-15　完成连接向导



图 5-16　连接 ADSL

任务 5.2　利用 FTP 服务器完成文件的下载和上传

任务描述：使用浏览器浏览 Web 页面，可以获得分布于世界各地服务器上的多种信息资源。但并不是 Internet 上所有的资源都以 Web 页面的形式存在，很多共享软件、免费程序、学术文献、影像资料等存放在公司、政府、大学的 FTP 服务器上，获得这些资源主要通过文件传输(FTP)服务。在 Internet 上下载到自己所需要的资料是用户生活中所必须具备的技能。要求通过下面的学习，能够掌握登录到 FTP 服务器，并完成文件的下载和上传的操作。

5.2.1　互联网的服务与应用

Internet 借助于现代通信手段和计算机技术实现了全球的信息传递。在 Internet 上，有各种虚拟的图书馆、商店、文化站和学校等，用户可以通过网络方便地获得或传送各

种形式的信息。就当前的发展现状而言，Internet 可以提供下述几种服务。

1. 电子邮件服务（E-mail）

电子邮件是 Internet 上使用最广泛的一种服务，也是 Internet 最基本的功能之一。它是一种通过计算机网络与其他用户进行联系的方便、快捷和价格低廉的现代化通信手段。电子邮件通过 Internet 上的邮件服务器实现收、发信双方的邮件传递。邮件服务器充当“邮局”的角色，用户可以在这台计算机上租用一个虚拟的电子信箱，当需要和网络上的其他人通信时，就可以通过电子信箱收、发信件。使用电子邮件的用户都可以通过各自的计算机编辑文件或信件，通过网络传送到对方的电子信箱中，而收件人则可以方便地进入 E-mail 系统读取自己信箱中的文件或信件。发信人可以一信多投，只需同时输入几个电子邮件地址即可，不必复制信的内容；收信人在阅读完信件后，可以直接将信件转发给他人。通过电子邮件，既可以传递文字和图片，也可以传递声音和图像。

2. 远程登录服务（Telnet）

远程登录服务用于在网络环境下实现资源的共享。利用远程登录，可以将自己的计算机暂时变成远程计算机的终端，从而直接调用远程计算机的资源和服务。在远程计算机上登录的前提是必须成为该系统的合法用户并拥有相应的 Internet 账户和口令。利用远程登录，用户可以实时使用远程计算机上对外开放的全部资源，例如查阅世界各地通过 Telnet 对外提供联机检索服务的图书馆中的藏书或研究机构中的数据等。此外，用户还可以在自己的计算机上发出命令来运行其他计算机上的软件。Internet 的许多服务都是通过 Telnet 访问来实现的。

3. 文件传输服务（FTP）

文件传输服务是 Internet 的传统服务项目之一，Internet 上有许多文件服务器，可以提供人们下载其上的信息资源，还可以提供存储空间供使用者将自己的文件传到文件服务器上。通过文件传输服务，用户不但可以获取 Internet 上丰富的资源，也可以将自己计算机中的文件传输到其他计算机中。所传输的内容可以是文字信息，也可以是非文字信息，包括计算机程序、图像、照片、音乐和影视等。此外，文件传输服务还提供登录、目录查询、文件操作及其他会话控制功能。

4. 信息查询服务

在 Internet 上，信息资源相当丰富，用户想要查询一条需要的信息时，可能要花费相当多的时间和精力。因此，Internet 提供了能在数台计算机上查找所需信息的工具，在此基础上，又开发出了一些功能完善、用户界面良好的信息查询工具来帮助用户更容易、更方便地获得所需的信息。这些查询工具有 Gopher、Archie 和 Wais 等。

（1）Gopher 是一种菜单驱动的信息查询工具，采用客户机/服务器的模式为用户服务。在 Internet 上有上千个 Gopher 服务器，它们将 Internet 上的信息资源组织成一个单一形式的资料库，使用关键字作为索引，使用户可以方便地从一台主机连接到另一台主机，快速查找所需要的资料。

（2）Archie 是一种文档查询服务工具，可以帮助用户在遍及全球的 FTP 服务器上查找到所需的文件。只要指定了要查找文件的检索关键字，Archie 就会查找包含该检索关键字的文件或目录，并将一一列出存储这些文件的 FTP 主机名称。

(3) Wais又称为广域信息服务系统,是一种快速查询信息的服务工具。它将相关的资料组织成为一个可以按照关键字检索的数据库,提供给公众检索。

5. 信息讨论及发布服务

Internet有着成千上万的用户。一些志同道合的用户可以组织起来,形成一个用户群,组成一些专题讨论小组。讨论涉及的内容相当广泛,有计算机、社科、天文、地理、时事和幽默等各种各样的专题。信息讨论和发布服务为人们相互联系、交流信息和观点提供了理想的场所,用户可以在此阅览他人发布的信息和观点,也可以发布自己的信息和观点。

6. 娱乐及会话服务

通过Internet这个巨大的网络系统,用户可以同世界各地的Internet用户进行实时通话,通过一些专门的设备,甚至可以传递音频和视频。此外,还可以参与各种游戏和娱乐,如网上棋牌大战,通过网络观看影片等。

5.2.2 文件传输服务FTP

1. FTP概述

在Internet中,文件传输是一种高效、快速传输大量信息的方式,它通过网络可以将文件从一台计算机传输到另一台计算机。文件传输协议FTP(File Transfer Protocol)是因特网上使用最广泛的协议,采用典型的客户机/服务器工作模式。客户机程序把客户的请求告诉服务器,并将服务器发回的结果显示出来。服务器执行真正的工作,如存储、发送文件等。

文件传输协议负责将文件从一台计算机传输到另一台计算机上,并且保证其传输的可靠性。该协议可以使不同类型的计算机之间通过网络实现文件的传输,并且可以传输不同类型的文件。

文件传输服务是一种实时的联机服务。FTP客户端程序必须与远程的FTP服务器建立连接并登录后,才能进行文件传输。通常一个用户必须在FTP服务器进行注册,拥有合法的用户名和密码后,才有可能进行有效的FTP连接和登录。

客户端在访问文件传输服务器时,启动本地计算机上的文件传输的客户端应用程序,输入用户名和密码;远处服务器响应客户端的登录请求,启动FTP服务器端程序,对客户的用户名和密码进行验证;如果用户密码正确,客户端即可登录到FTP服务器,从而建立起连接,进行文件的传输。

在这里,首先必须分清文件传送(file transfer)和文件存取(file access)之间的区别。由FTP提供的文件传送是将一个完整的文件从一个系统复制到另一个系统中。在FTP服务中,用户经常遇到两个概念:“下载”和“上传”。下载服务:服务器端响应客户端的请求,将服务器上的文件复制到客户端的计算机上的过程。上传服务:客户端将本地计算机上的文件复制到文件传输服务器上的过程。用Internet语言来说,用户可通过客户机程序向(从)远程主机上传(下载)文件。文件存储是应用系统(如NFS等)提供的。

使用FTP时必须首先登录,在远程主机上获得相应的权限以后,方可上传或下载文件。也就是说,要想同哪一台计算机传送文件,就必须具有那一台计算机的适当授权。换

言之,除非有用户 ID 和口令,否则便无法传送文件。这种情况违背了 Internet 的开放性,Internet 上的 FTP 主机何止千万,不可能要求每个用户在每一台主机上都拥有账号。匿名 FTP 就是为解决这个问题而产生的。匿名 FTP 服务的实质是:提供服务的机构在它的 FTP 服务器上建立一个公开账户(一般为 anonymous),并赋予该账户访问公共目录的权限,以便提供免费服务;要访问提供匿名服务的 FTP 服务器,一般不需输入用户名与密码。如果需要,可以使用 anonymous 作为用户名,使用有效的 E-mail 地址或 guest 作为用户密码;为了保证 FTP 服务器的安全,几乎所有匿名 FTP 服务器都只允许用户下载文件,而不允许用户上传文件。

2. FTP 工作原理

早期,Internet 上实现文件传输并不是一件容易的事。Internet 是非常复杂的网络,连接在 Internet 上的计算机已有上千万台,而这些计算机可能运行不同的操作系统,有运行 UNIX 的服务器,也有运行 DOS、Windows 的 PC 和运行 MacOS 的苹果机等,而各种操作系统之间的文件交流问题,需要建立一个统一的文件传输协议,这就是所谓的 FTP。基于不同的操作系统有不同的 FTP 应用程序,而所有这些应用程序都遵守同一种协议,这样用户就可以把自己的文件传送给别人,或者从其他的用户环境中获得文件。

FTP 使用客户端/服务器方式;一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成:一个主进程,负责接收新的请求;另外有若干个从属进程,负责处理单个请求。以传文件为例介绍 FTP 协议的工作过程。

主进程的工作步骤如下:

(1) 打开熟知端口(端口号为 21),迎接客户端进程的连接。

(2) 等待客户端进程发出连接请求。

(3) 启动从属进程来处理客户端进程发来的请求。从属进程对客户端进程的请求处理完后即终止,但从属进程在运行期间根据需要还可能创建其他一些子进程。

(4) 回到等待状态,继续接收其他客户进程发来的请求。主进程与从属进程的处理是并发进行的。图 5-17 描述了客户与服务器以及它们之间的连接情况。

从图 5-17 中可以看出,FTP 在客户端和服务器之间建立了两个连接:控制连接和数据连接。控制连接用于传送客户端与服务器之间的命令以及相应的回送信息,数据连接用于客户端与服务器之间的数据交换。交互式用户通常不处理在控制连接中转换的命令和应答,这些细节均由两个协议解释器来完成。标有“用户接口”的方框,功能是按用户所需提供各种交互界面(全屏幕菜单选择,逐行输入命令等),并把它们转换成在控制连接上发送的 FTP 命令。类似地,从控制连接上传回的服务器应答也被转换成用户所需的交互格式。从图 5-17 中还可以看出,正是这两个协议解释器根据需要激活文件传送功能。

3. FTP 的工作方式

FTP 支持两种模式:一种方式叫做 Standard (也就是 Port 方式,主动方式);另一种方式是 Passive(也就是 PASV,被动方式)。Standard 模式 FTP 的客户端发送 Port 命令到 FTP 服务器。Passive 模式 FTP 的客户端发送 PASV 命令到 FTP 服务器。

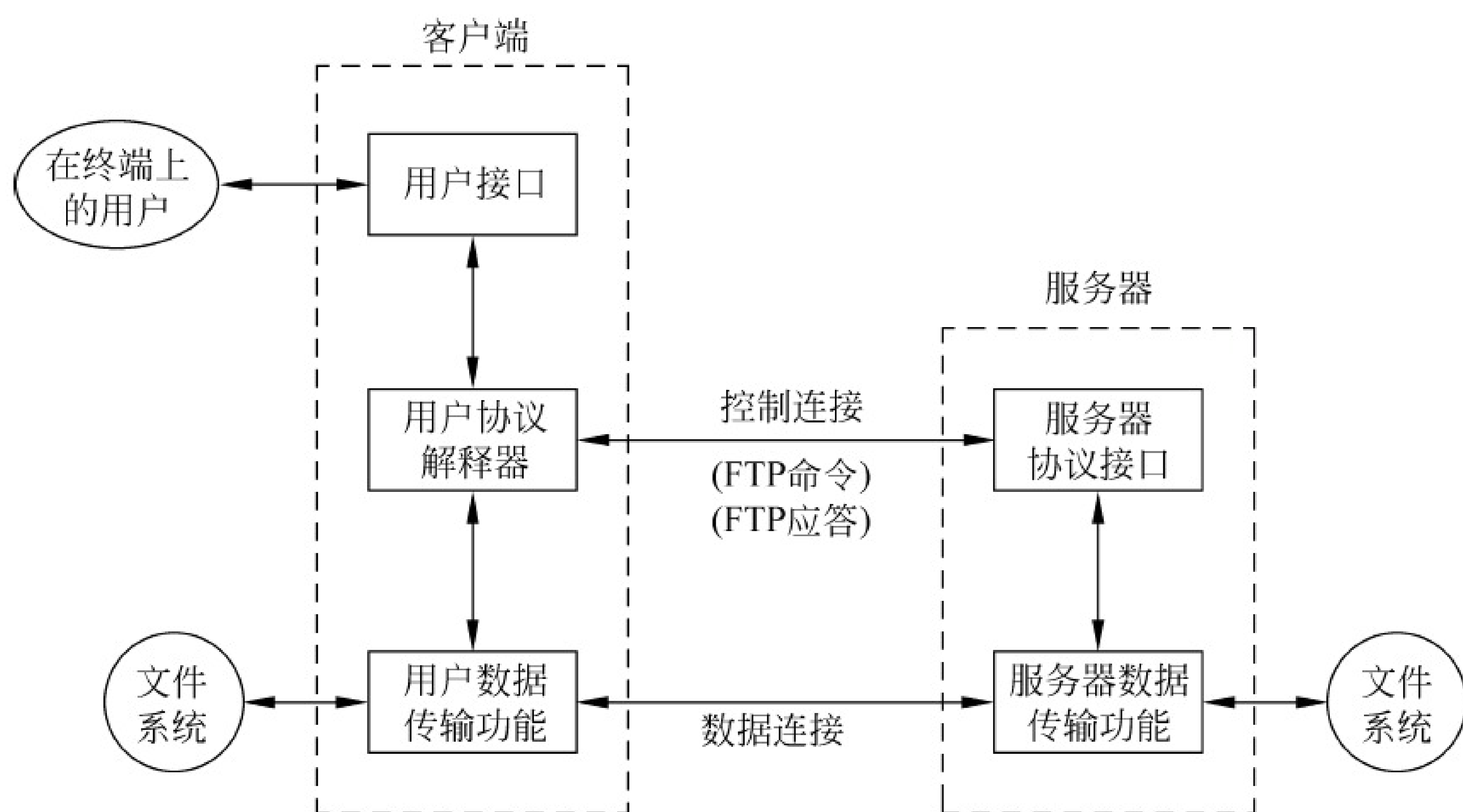


图 5-17　FTP 原理示意图

下面介绍这两种方式的工作原理。

(1) Standard 模式

FTP 客户端首先和 FTP 服务器的 TCP 21 端口建立连接,通过这个通道发送命令,客户端需要接收数据时在这个通道上发送 Port 命令。Port 命令包含了客户端用什么端口接收数据。在传送数据的时候,服务器端通过自己的 TCP 20 端口连接至客户端的指定端口发送数据。FTP 服务器端必须和客户端建立一个新的连接用来传送数据。

(2) Passive 模式

在建立控制通道的时候和 Standard 模式类似,但建立连接后发送的不是 Port 命令,而是 PASV 命令。FTP 服务器收到 PASV 命令后,随机打开一个高端端口(端口号大于1024)并且通知客户端在这个端口上传送数据的请求,客户端连接 FTP 服务器此端口,然后 FTP 服务器将通过这个端口进行数据的传送,这个时候 FTP 服务器不再需要建立一个新的和客户端之间的连接。

很多防火墙在设置的时候都是不允许接受外部发起的连接的,所以许多位于防火墙后或内网的 FTP 服务器不支持 PASV 模式,因为客户端无法穿过防火墙打开 FTP 服务器的高端端口;而许多内网的客户端不能用 Port 模式登录 FTP 服务器,因为从服务器的 TCP 20 无法和内部网络的客户端建立一个新的连接,造成无法工作。

4. FTP 服务器的访问方法

FTP 是基于客户机/服务器结构而设计的。FTP 服务器的访问形式有两种:Web 页面形式的文件传输服务和独立的 FTP 服务。

(1) Web 页面形式的文件传输服务

由于 Web 页面的友好性,FTP 服务采用 Web 页面的形式为用户提供文件传输服务。这是目前 Internet 上 FTP 服务器的常见形式。Web 页面形式的文件传输也有两种形式。

① 在浏览器窗口的地址栏中输入 FTP 服务器的地址,然后输入登录的用户名和密码。如图 5-18 所示,以匿名方式访问 FTP 服务器的操作。



图 5-18　微软的匿名 FTP 服务器窗口

② 在 FTP 服务商提供的 Web 页面中单击相关链接，实现文件的下载，但是这类 FTP 服务器一般只能提供文件下载，无法实现文件上传的功能。

(2) 独立的 FTP 服务

对于独立的 FTP 服务，必须使用专门的 FTP 命令或称 FTP 软件，输入已注册的用户名和口令后，才能连接到 FTP 服务器上，从而实现文件传送的任务。常用的 FTP 软件有系统自带的 Ftp.exe、CuteFTP、LeapFTP、Ws-FTP 等，这些软件的原理基本相同，只是功能和界面略有不同。下面以 Windows 的 FTP 命令为例，介绍使用独立的 FTP 服务的方法。

① 启动 FTP 命令

选择"开始"→"运行"命令，输入"ftp"，单击"确定"按钮，出现 FTP 命令窗口。在该窗口中命令提示符是 ftp>，表明正在运行的 FTP 命令。

② 与 FTP 服务器建立连接

使用某个 FTP 服务器提供的功能之前，先要使用 open 命令与 FTP 服务器建立连接。例如：

```
ftp>open 10.4.8.101
```

命令输入后，FTP 命令将和 IP 地址为 10.4.8.101 的 FTP 服务器进行连接，如果连接成功则会显示如图 5-19 所示的信息。

③ FTP 目录与文件操作

在 FTP 服务器上有许多目录与文件，有一系列命令可以对这些目录或文件进行操作，从而可以查看目录列表、修改目录、下载文件、上传文件等各项操作。各命令的使用和功能如下。

PWD 命令：用于显示 FTP 服务器的当前工作目录。格式为"ftp>pwd"。

LS 命令：显示 FTP 服务器上当前目录下的文件与子目录名称。

DIR 命令：显示 FTP 服务器上当前目录下的文件与子目录名称。与 LS 目录在显示格式上不同，更详细一些。



图 5-19 与 FTP 服务器建立连接后的窗口

CD 命令：改变 FTP 服务的当前目录。命令格式为“ftp>cd 目录路径”。

LCD 命令：用于改变本地计算机的当前目录。命令格式为“fpt>lcd 目录路径”。

GET 命令：用于下载文件，即将 FTP 服务器上的一个文件传输到本地计算机上。命令的使用格式是“ftp>get 源文件名［目标文件名］”。

MGET 命令：用于下载多个文件，命令的使用格式是“ftp>mget 文件列表”。命令中的文件列表是指用空格分隔的多个文件的序列。可以使用通配符“*”和“?”来代表多个或一个字符。

PUT 命令：可以将本地计算机上的一个文件传输到 FTP 服务器上。命令的格式是“ftp>put 源文件名［目标文件名］”。

MPUT 命令：用于将多个文件上传到 FTP 服务器上。格式是“mput 文件列表”。与 MGET 命令一样，文件列表是指用空格分隔的多个文件名的序列，也可以使用通配符。

BINARY 命令和 ASCII 命令：用来改变传输文件的模式。如果要传输可执行的二进制文件，使用 BINARY 命令先改变模式。如果要传输文本文件，先用 ASCII 命令改变模式。

5.2.3 电子邮件服务

1. E-mail 基础知识

电子邮件（E-mail）是因特网上使用得最多的和最受用户欢迎的一种应用。电子邮件将邮件发送到 ISP 的邮件服务器，并放在其中的收信人邮箱（Mail Box）中，收信人可随时上网到 ISP 的邮件服务器进行读取。相当于利用因特网为用户设立了存放邮件的信箱。因此 E-mail 有时也称为“电子信箱”。电子邮件不仅使用方便，而且还具有传递迅速和费用低廉的优点。据有的公司报道，使用电子邮件后可提高劳动生产率 30% 以上。现在电子邮件不仅可传送文字信息，而且还可以附上声音和图像。由于电子邮件的广泛使用，现已很少有人愿意到邮局发电报，因为这种传统电报既贵又慢又不方便。

(1) 电子邮件的发展历程

20 世纪 70 年代，美国 ARPA 的科研人员在进行 Internet 的项目研究时，为了方便科研人员之间通信，便想到利用计算机网络作为一种个人之间的通信方式。

1982 年，ARPA 的“E-mail 建议”作为 RFC(评议请求)的 821 号文件和 822 号文件公开出版。计算机局域网的蓬勃发展，促进了电子邮件系统的应用范围迅速扩大。

以后，国际电报电话咨询委员会 CCITT 也决定介入电子邮件业务，为此草拟了 X.400 建议。由于全世界的电话网络已经有统一标准，不同国家之间的电话系统可以互操作，所以，人们只要在自己的计算机上加上一个调制解调器和一套通信软件，便可以利用电话线进行通信。这样，E-mail 系统便从美国本土很快地推广到全世界。另外，美国的贝尔实验室成功解决了与调制解调器通信的所有技术问题。

(2) 电子邮件系统的组成

电子邮件系统是一种存储转发系统。当一封邮件发出后，首先由 Internet 上的某台计算机接收该邮件(存储)，然后该计算机经过地址识别，选择一条最佳路径发送到下一个 Internet 上的计算机(转发)，直到到达目的地址。

一个电子邮件系统应具有如图 5-20 所示的三个主要组成构件，这就是用户代理，邮件服务器，以及电子邮件使用的协议，如 SMTP 和 POP3(IMAP)等。在图 5-20 中只画出 POP3。

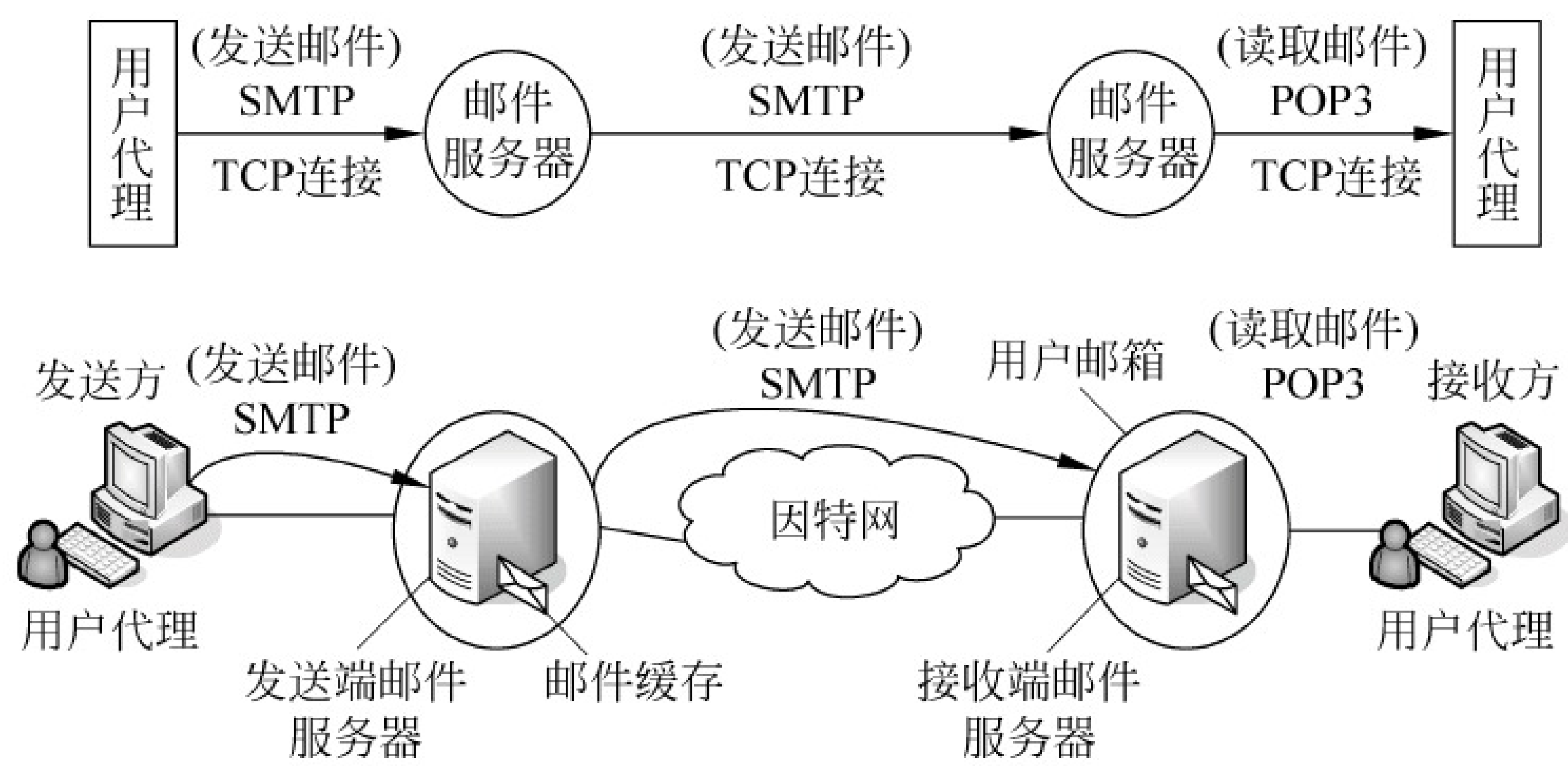


图 5-20　电子邮件系统

用户代理 UA(User Agent)是用户与电子邮件系统的接口。在大多数情况下它就是在用户 PC 中运行的程序。用户代理使用户能够通过一个很友好的接口(目前主要是用窗口界面)来发送和接收邮件。

邮件服务器是电子邮件系统的核心构件。因特网上所有的 ISP(网络服务提供商)都有邮件服务器。邮件服务器的功能是发送和接收邮件，同时还要向发信人报告邮件传送的情况(已交付、被拒绝、丢失等)。邮件服务器按照客户机/服务器方式工作。邮件服务器需要使用两个不同的协议。负责发送邮件的系统，采用的是简单邮件传送协议，即 SMTP 协议，担任这一部分功能的服务器就叫做 SMTP 服务器；负责检索并接收邮件的系统，采用的是邮局协议，即 POP(Post Office Protocol)协议，担任这一部分功能的服务器叫做 POP3 服务器。通常来说，SMTP 服务器与 POP3 服务器使用的是同一台服务器。

这里应当注意：一个邮件服务器既可以作为客户机，也可以作为服务器。例如，当邮件服务器A向另一个邮件服务器B发送邮件时，邮件服务器A就作为SMTP客户，而B是SMTP服务器。当邮件服务器A从另一个邮件服务器B接收邮件时，邮件服务器A就作为STMP服务器，而B是SMTP客户端。

（3）电子邮件的相关协议

① 简单邮件传输协议SMTP

简单邮件传输协议SMTP包括两个子集：一个是标准子集定义电子邮件信息的格式；另一个是传输邮件的标准子集。SMTP的主要任务是负责服务器之间的邮件传送。它的最大特点就是简单，因为它只规定了电子邮件如何在Internet中通过TCP协议在发送方和接收方之间进行传送，诸如与用户的交互、邮件的存储、邮件系统发送邮件的时间间隔等操作均不涉及。

在电子邮件系统中，发信方的主机为客户方，收件人的邮件服务器为服务方，双方机器上的SMTP协议相互配合，将电子邮件从发信方的主机传送到收信方的信箱中。SMTP使用TCP协议连接，默认端口号是25。

② 邮局协议POP3

POP3的主要任务是当用户计算机与邮件服务器连通时，将邮件服务器的电子邮箱中的邮件直接传送到用户计算机上。

用户激活一个POP3客户，该客户创建一个TCP连接，送到用户邮箱所在的POP3服务器。用户首先发送登录名和口令，以鉴别该会话。一旦接受了鉴别，用户就可以发送命令，检索一个或多个邮件的副本，或者从邮箱中删除邮件。

③ 因特网信息访问协议IMAP

IMAP提供了一个在远程服务器上管理邮件的手段，允许用户使用电子邮件服务器上的电子邮件和公告栏信息。IMAP具有智能邮件存储功能，用户可以在下载邮件前预览信息，包括是否下载附件等。用户可以使用服务器上的过滤软件或搜索代理软件，可以从任何地方、任何机器上获取邮件信息。IMAP具有远程访问的能力，用户阅读服务器上的邮件，就像邮件存储在本机上一样。IMAP与POP相比，增加了只下载邮件的标题、建立多个邮箱和在服务器上建立保存邮件的文件夹等功能。

④ 多用途网际邮件扩展协议MIME

该协议是IETF于1993年通过的一个电子邮件标准，是为了使因特网用户能够传送二进制数据而制定的标准。MIME能满足人们对多媒体电子邮件和使用本国语言发送邮件的需求。MIME邮件信息格式的邮件体中不仅允许ASCII码文本信息，而且允许8位文本信息以及图像、语音等非文本的二进制信息。

2. 电子邮件地址的格式

电子邮件与普通信件一样，通过计算机发送时均需要写上发信人和收信人的地址，一般称为“E-mail地址”，或者“电子邮件地址”。所有的Internet上的用户一般都具有一个或几个信箱地址，一个地址只能对应于一个用户，但是一个用户却可以有几个信箱地址。E-mail地址由用户名和邮件服务器的主机名（包括域名）组成，中间用@分隔，其格式如下：

用户名@主机名.域名

这里,@表示"在"(即英文单词 at),是电子邮件地址的标志。在它的左边为用户名,也就是用户的账号,是用户在注册邮箱时所取的名字;在它的右边由主机名和域名组成。

3. 电子邮件信息格式

SMTP 协议规定电子邮件的信息由封皮、邮件头和邮件体组成。

(1)封皮

封皮包括发信人和收信人的电子邮件地址。邮件服务器使用它来传输电子邮件。

(2)邮件头

客户端的邮件应用程序处理邮件头,并将邮件头信息显示给用户。邮件头提供了详细的技术信息,包括发信人、收信人、发信日期和时间、信件的主题等。

例如,2008年7月26日,Chen 从中国给在美国读书的 Zhao 发去一封表示感谢她帮助的邮件,并抄送给在英国的 Wang。其中,Chen 的 E-mail 地址是:Chen@public.Intercom.com.cn,Zhao 的 E-mail 地址是:zhaowz@gmail.com,Wang 的 E-mail 地址是:Wang@sussex.ac.uk,那么,这个电子邮件的邮件头格式如下所示。

发件人:Chen@public.Intercom.com.cn(发信人的 E-mail 地址)

收件人:zhaowz@gmail.com(收信人的 E-mail 地址)

抄送:Wang@sussex.ac.uk(抄送第三者的 E-mail 地址)

主题:Thanks(邮件的主题内容)

日期:Fri.26 Jan. 2005 12:28:01(信件发出的日期和时间)

(3)邮件体

邮件体是邮件的内容,是用户要传送的信息。

4. 电子邮件的收发过程

电子邮件系统是 Internet 上一种典型的客户机/服务器(Client/Server)系统。接收与发送电子邮件的过程如下。

(1)发件人在本地的计算机上启动电子邮件客户端软件,或者直接用浏览器软件登录电子邮件服务器,编辑好一封邮件发送出去。

(2)邮件首先被传送到发件人的 SMTP 服务器,SMTP 服务器负责将邮件发送到由收件人指定的邮件服务器上。

(3)收件人进入到因特网后,启动其电子邮件客户端软件或者使用浏览器登录电子邮件服务器,就可以通过 POP3 服务器将邮件接收到自己的计算机上。

如果电子邮件由于地址错误或者其他原因无法送达收件人的邮件服务器,SMTP 服务会自动将原信退回发件人,并附加上无法送达的原因。

5. 申请免费的电子信箱

因特网上提供免费电子邮箱服务的很多,国内比较知名的网站,如新浪、搜狐、网易、雅虎等都为用户提供免费电子邮件服务。尽管在运行速度,空间大小,稳定性上良莠不齐。但对于一般使用者来说,多数免费电子信箱是能够满足要求的。下面介绍如何申请雅虎免费中文电子邮箱,供初涉因特网的朋友参考。

(1)登录 Yahoo 免费邮箱网站。在 IE 浏览器地址栏输入免费电子邮箱的网址 mail.

yahoo.com.cn。目前 Yahoo 提供 1GB 大小的免费电子邮箱空间。如图 5-21 所示。



图 5-21 雅虎邮箱

(2) 单击页面上的“注册新邮箱”按钮，进入账号注册申请页面，如图 5-22 所示。在邮箱地址文本框中输入一个邮箱地址的账号名，如“ilumail_2006”，单击“下一步”按钮。



图 5-22 注册邮箱：邮箱地址

(3) 进入密码设置页面，如图 5-23 所示。在填写的过程中，注意文本框后面带有 * 号的项目必须填写，填完注册信息后，单击页面中的“完成”按钮，于是就申请到了一个免费的电子邮箱。

注意：申请免费的电子邮箱后，用户应将该邮箱的 SMTP 和 POP3 服务器的地址记录下来，为以后配置电子邮件软件(如 Outlook 等)做好准备。

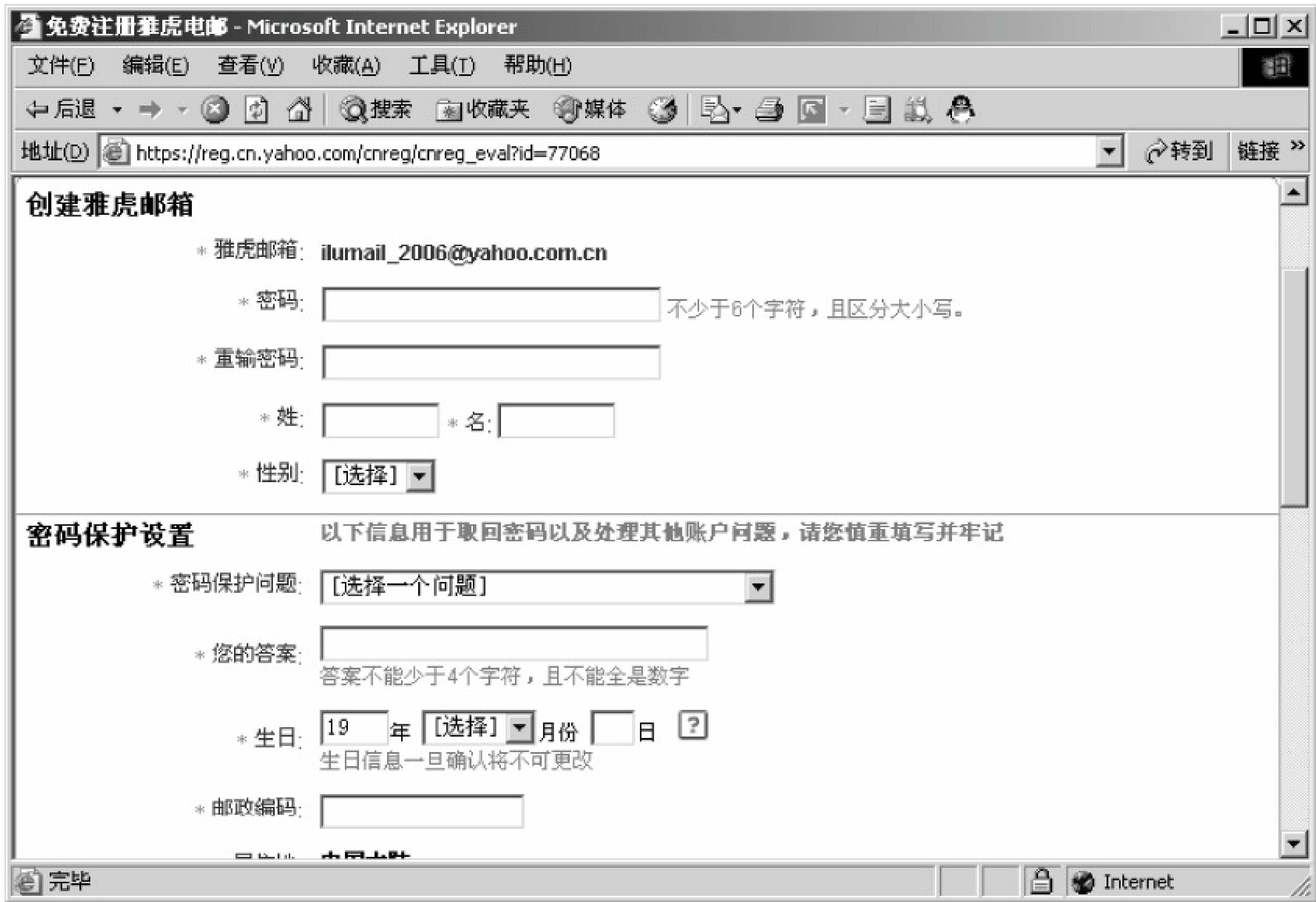


图 5-23　注册邮箱：基本信息

6. 以 Web 方式收发电子邮件

（1）登录 Web 邮件系统

在如图 5-21 所示的页面中输入刚申请成功的邮件账号 ilumail_2006 和密码，然后单击“登录”按钮。进入如图 5-24 所示的页面。



图 5-24　登录 Yahoo Web 邮件系统

(2) 使用 Web 邮件系统收发电子邮件

① 写信并发送邮件

在如图 5-24 所示的页面中,单击"写信"按钮,进入如图 5-25 所示的页面。

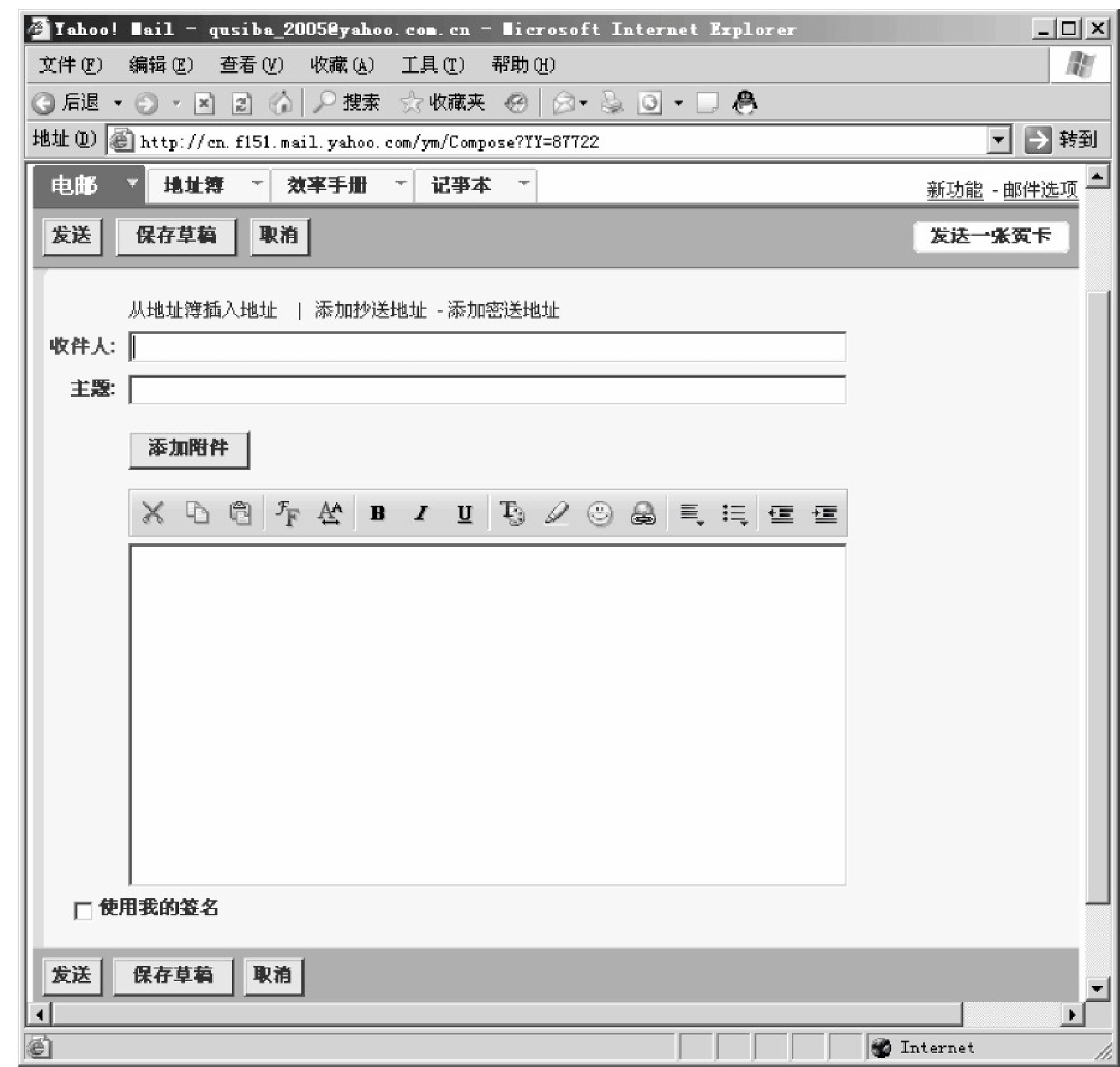


图 5-25 邮件撰写页面

在收件人中输入 ilumail_2006@yahoo.com.cn,主题栏输入邮件的主题,如"测试邮件"。如果有附件,单击"添加附件"按钮,进行附件的添加,添加完附件后,单击"回到原邮件"按钮。然后输入邮件正文内容,正文内容部分可以使用 HTML 编辑器插入表格或图片。写完后的邮件如图 5-26 所示。单击图中的"发送"按钮,即可完成邮件的发送。

② 收阅信件

单击如图 5-24 所示的"收件箱"超链接,可打开如图 5-27 所示的收件箱页面。

可以看到,刚才给自己发送的一封电子邮件现在已经收到了。单击主题为"测试邮件"的超链接,即可打开并阅读此封邮件,如图 5-28 所示。

③ 回复或转发邮件

在如图 5-28 所示的页面中,可直接单击"回复"按钮给发件人发回信。或单击"转发"按钮对邮件进行转发。



图 5-26　撰写完成的邮件



图 5-27　收件箱



图 5-28　阅读邮件

7. 使用电子邮件软件收发邮件

除了 Web 方式外，用户也可以在计算机上安装一个进行电子邮件处理的客户程序，如 Windows XP 里的 Exchange，专用程序 Eudora 等。本书以 Microsoft Internet Explorer 6.0 软件包中的 Outlook Express 程序为例讲述电子邮件软件的有关操作。

在用户的计算机中安装 IE 6.0 软件包后，执行“开始”→“程序”→Outlook Express 命令，启动电子邮件客户程序 Outlook Express。

Outlook Express 主要使用以下几个文件夹对邮件进行管理：

“收件箱”文件夹下保存用户收到的电子邮件。

“发件箱”文件夹下保存已撰写完毕等待发送的电子邮件。

“已发送邮件”文件夹下保存已发送出去的电子邮件。

“已删除邮件”文件夹下保存在其他文件夹下被删除的邮件。

“草稿”文件夹下保存撰写了一部分需要以后修改使用的邮件。

用 Outlook Express 收发邮件前要在程序中设置一个邮件账号。设置邮件账号的过程包括设置用户邮件地址、用户邮件服务器名称等信息。

（1）设置电子邮件账户

① 添加一个邮件账号

在 Outlook Express 窗口中，执行“工具”→“账号”命令，出现如图 5-29 所示的对话

框。单击对话框中的“邮件”标签，主窗口中将显示出客户程序中已设置的所有邮件账号。

单击“添加”按钮，选择菜单项“邮件”，得到图 5-30 所示的画面。



图 5-29　添加邮件账号



图 5-30　输入用户姓名

② 输入用户显示名称

在如图 5-30 所示的对话框中，输入用户的显示名称，单击“下一步”按钮，得到如图 5-31 所示的对话框。用户的显示名称是用户在发送电子邮件时自动显示在邮件中的用户名称，设置成什么名称并不影响邮件的发送，一般都设置成自己的真实姓名。

③ 输入 E-mail 地址

在如图 5-31 所示的对话框中，选择“我想使用一个已有的电子邮件地址”，在“电子邮件地址”文本框中输入用户的 E-mail 地址，单击“下一步”按钮。得到如图 5-32 所示的界面。



图 5-31　输入电子邮件地址



图 5-32　设置邮件服务器

④ 输入服务器信息

在如图 5-32 所示的对话框中，在“我的邮件接收服务器是”中选择 POP3(除非用户的 ISP 告知用户应选 IMAP 类型)，并输入 POP3 服务器的名称和 SMTP 服务器的名称，单击“下一步”按钮，得到如图 5-33 所示的对话框。POP3 及 SMTP 服务器的名称是申请电

子信箱时 ISP 提供给用户的。

⑤ 输入邮件账号和密码

在如图 5-33 所示的对话框中,输入邮件账号和密码,单击“下一步”按钮,得到如图 5-34 所示的对话框。邮件账号就是邮件地址中符号“@”前面的部分。密码是用户从 ISP 获知邮件地址的同时得到的,用来从 POP3 服务器接收电子邮件时进行身份验证。



图 5-33　邮件账号及密码



图 5-34　设置完成

⑥ 完成新邮件账号的设置

在如图 5-34 所示的对话框中,单击“完成”按钮,结束新邮件账号的设置。以后就可以用这个账号在 Outlook Express 中收发电子邮件了。

(2) 使用 Outlook Express 进行电子邮件的收发与阅读

① 撰写新邮件

单击 Outlook Express 窗口中的“新邮件”按钮,得到如图 5-35 所示的对话框,在窗口中输入一封新邮件的有关内容。邮件内容由两部分组成:一部分是邮件头,包括收件人、抄送、主题;另一部分是邮件正文。



图 5-35　写邮件

新邮件写完之后,单击图 5-35 中的“发送”按钮或执行菜单命令“文件”→“发送邮件”,将邮件发送出去;执行“文件”→“以后发送”,邮件被存入“发件箱”待以后发送;执行“文件”→“保存”命令,邮件被保存到“草稿”中;执行“文件”→“另存为”命令,邮件可存储到计算机的其他文件夹下。

② 发送邮件

编辑好新邮件后,可以单击图 5-35 对话框中工具栏上的“发送”按钮或执行菜单命令“文件”→“发送邮件”直接将邮件发送出去。也可以对保存在“收件箱”中的信件统一发送。在如图 5-36 所示对话框中用鼠标单击“发件箱”文件夹,对话框右边上半部分显示出当前“发件箱”中未发出的邮件,对话框右边下半部分显示出邮件目录中光标所在邮件的内容。



图 5-36　发件箱

要修改邮件的内容,可用鼠标双击邮件目录中的相应的邮件,在弹出的邮件撰写窗口中修改邮件内容。执行菜单命令"工具"→"发送和接收"→"发送全部邮件",程序开始发送"发件箱"中的所有邮件,发送过程中出现如图 5-37 所示的界面。已发送的邮件将从"发件箱"中消失并出现在"已发送邮件"中。

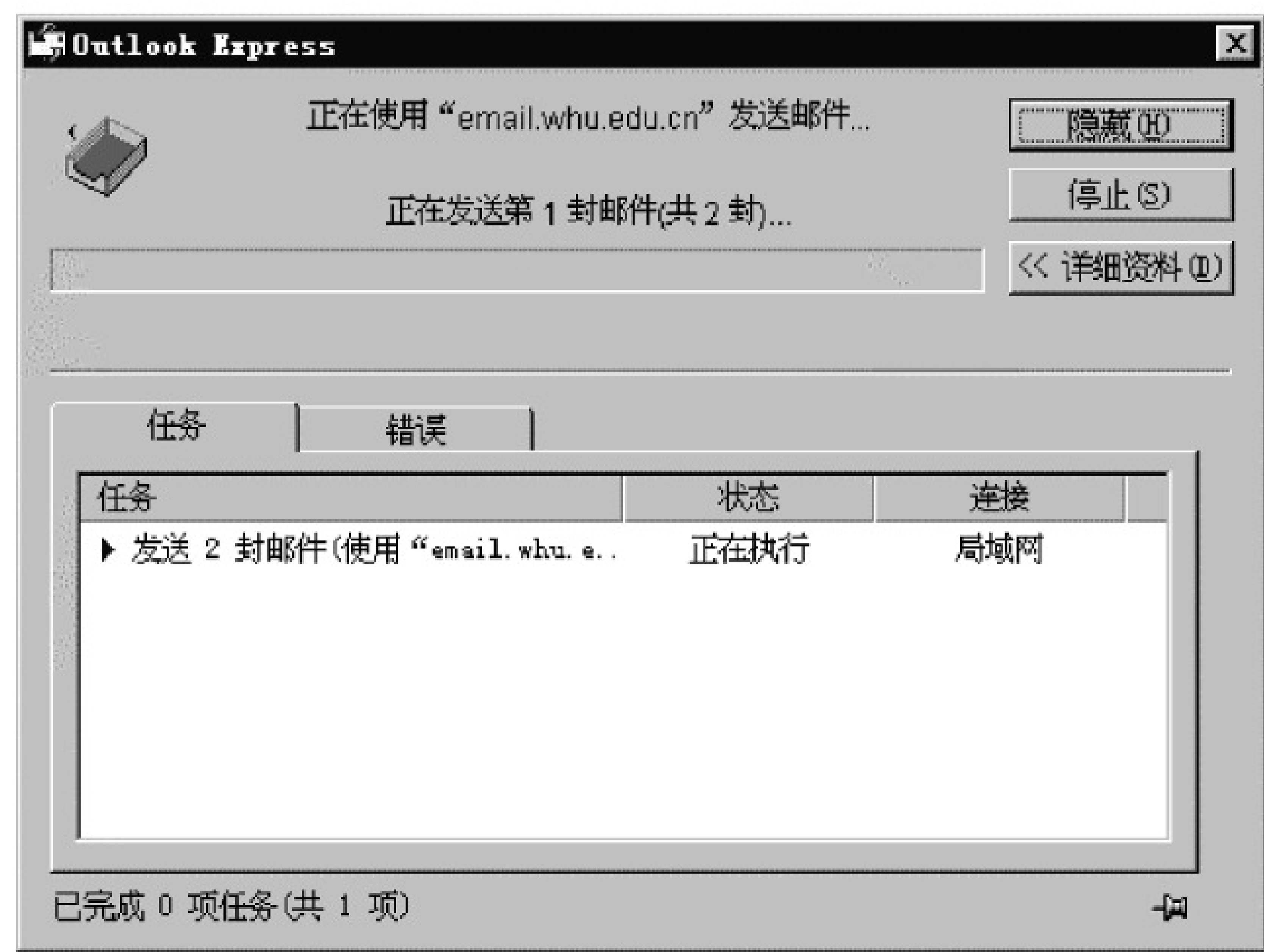


图 5-37　发送邮件

③ 接收新邮件

执行菜单命令"工具"→"发送和接收"→"接收全部邮件",程序进行新邮件接收工作。接收过程中出现如图 5-38 所示的界面。接收新邮件实际上是将邮件服务器上的新邮件下载到"收件箱"文件夹中。

④ 阅读邮件

用鼠标单击"收件箱"文件夹,如图 5-39 所示,窗口的右边分为上下两部分:上部分列出"收件箱"中所有的邮件目录;下面的部分列出当前光标所在邮件的内容。

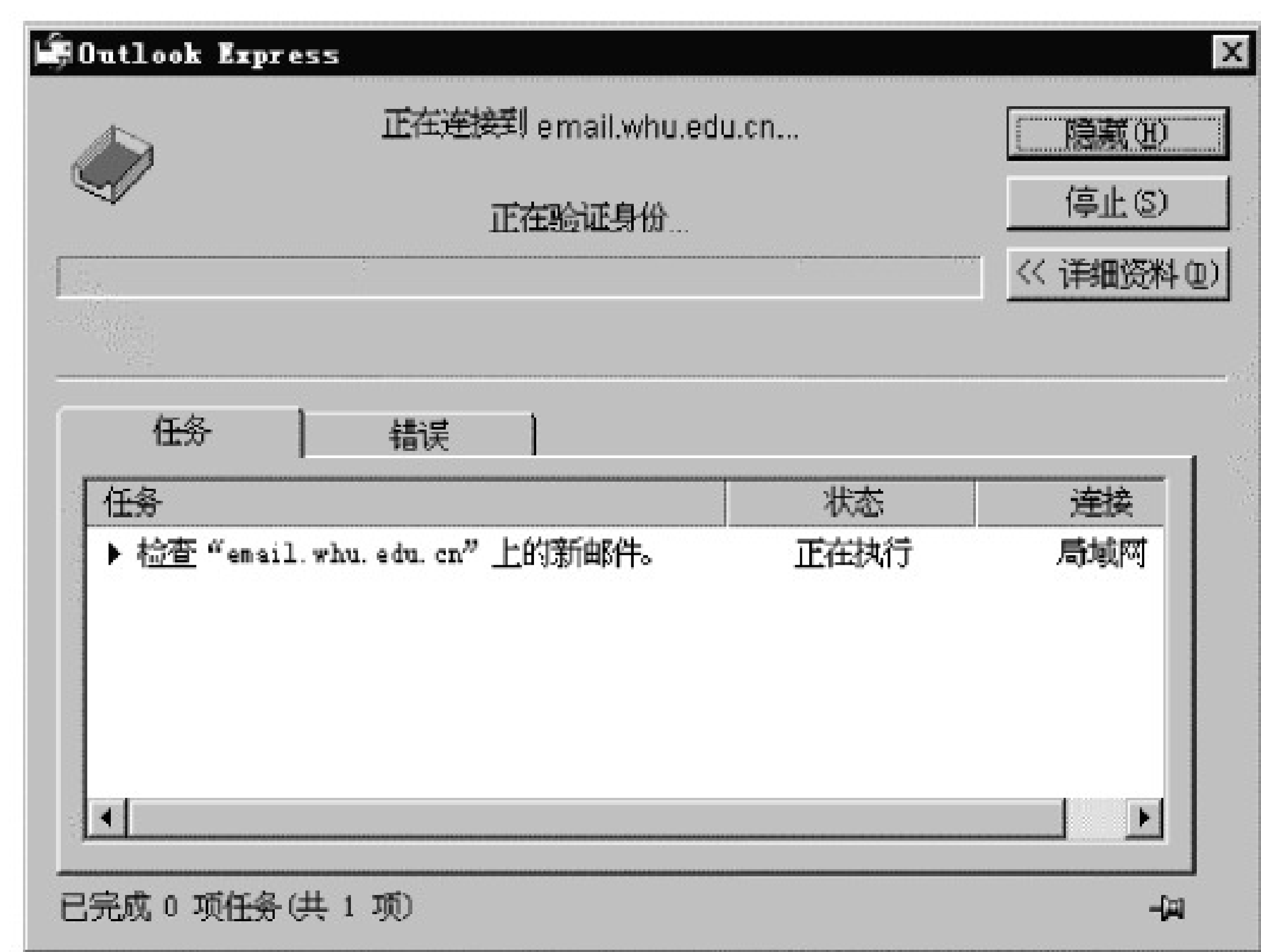


图 5-38　接收新邮件



图 5-39　阅读邮件

邮件目录前有一个信封状的小图标,如果小图标是合拢的则表示该邮件尚未阅读。通过浏览邮件目录的主题,可大致了解邮件的内容。如果要阅读某邮件,将光标移到该邮件目录上,右下窗口会显示出邮件的正文内容,或者双击邮件目录中的该邮件,然后在弹出的邮件窗口中阅读邮件。

⑤ 删除邮件

无论在哪个文件夹中,先将光标移到邮件目录中要删除的邮件上,再单击工具栏上的"删除"按钮,就会对邮件进行删除操作。需要注意的是,对"已删除邮件"文件夹中的邮件执行删除操作会真正使邮件从用户的计算机中删除,而对其他文件夹下的邮件执行删除操作只是将邮件移到"已删除邮件"文件夹中。

5.2.4　信息浏览与检索

Internet 的广泛应用和发展,使得全球范围的信息资源交流、共享成为可能,它为人们提供了一个广大的信息共享与检索的空间。Internet 已经成为全球范围内传播和交流科研、教育、商业和社会等各种信息的重要渠道之一。

用户必须使用基于 HTTP 协议的应用程序在 Internet 上浏览信息,这样的应用程序就是浏览器。浏览器的作用是向远程的 WWW 服务器发送服务请求,并将服务器处理请求的结果信息传输并显示到本地计算机上,对信息进行浏览及保存等操作。

世界上第一个浏览软件叫做 Mosaic,是 1993 年年初开发出来的。目前使用最广泛的浏览器软件是微软公司的 Internet Explorer(简称 IE)和网景公司(已被美国在线 AOL 收购)的 Netscape Navigator(简称 Netscape),另外,还有近年来较流行的 MyIE(现更名为傲游 Maxthon)等。

下面简单地介绍微软 Internet Explorer 6.0 浏览器软件的使用方法。

1. IE 的基本操作

只要安装了 Windows XP 系统 IE 浏览器就会自动安装,如果不打算使用 IE 了,可把它卸载。卸载的方法是通过 Windows"控制面板"中的"添加/删除程序"完成的。单击"添加删除程序"窗口中的"添加删除 Windows 组件"按钮,在组件列表框中将 Internet Explorer 复选框取消选择,单击"下一步"按钮,单击"完成"按钮,进行 IE 的卸载。如果以

后再使用按同样的步骤，选择复选框即可。

（1）启动 Internet Explorer

启动 IE 浏览器，可以单击桌面上的 IE 浏览器快捷方式图标，或者执行菜单命令“开始”→“程序”→Internet Explorer，也可以单击任务栏上的“启动 Internet Explorer”按钮。IE 浏览器窗口如图 5-40 所示。



图 5-40　IE 主界面

（2）使用 IE 访问 WWW 资源

浏览 Internet 上的信息，如果知道要浏览的信息资源的网页的地址，可以在打开 IE 浏览器的地址栏输入网址，然后按回车键，或单击“转到”按钮就可以进入相应的页面，浏览网页。如图 5-41 所示。



图 5-41　地址栏的使用

当某个网页被显示后，通过单击网页中的超级链接可以进入到相应的页面访问资源，如图 5-42 所示。网页中的超链接是当鼠标指向文字、图片或动画上时，指针会变成手形。

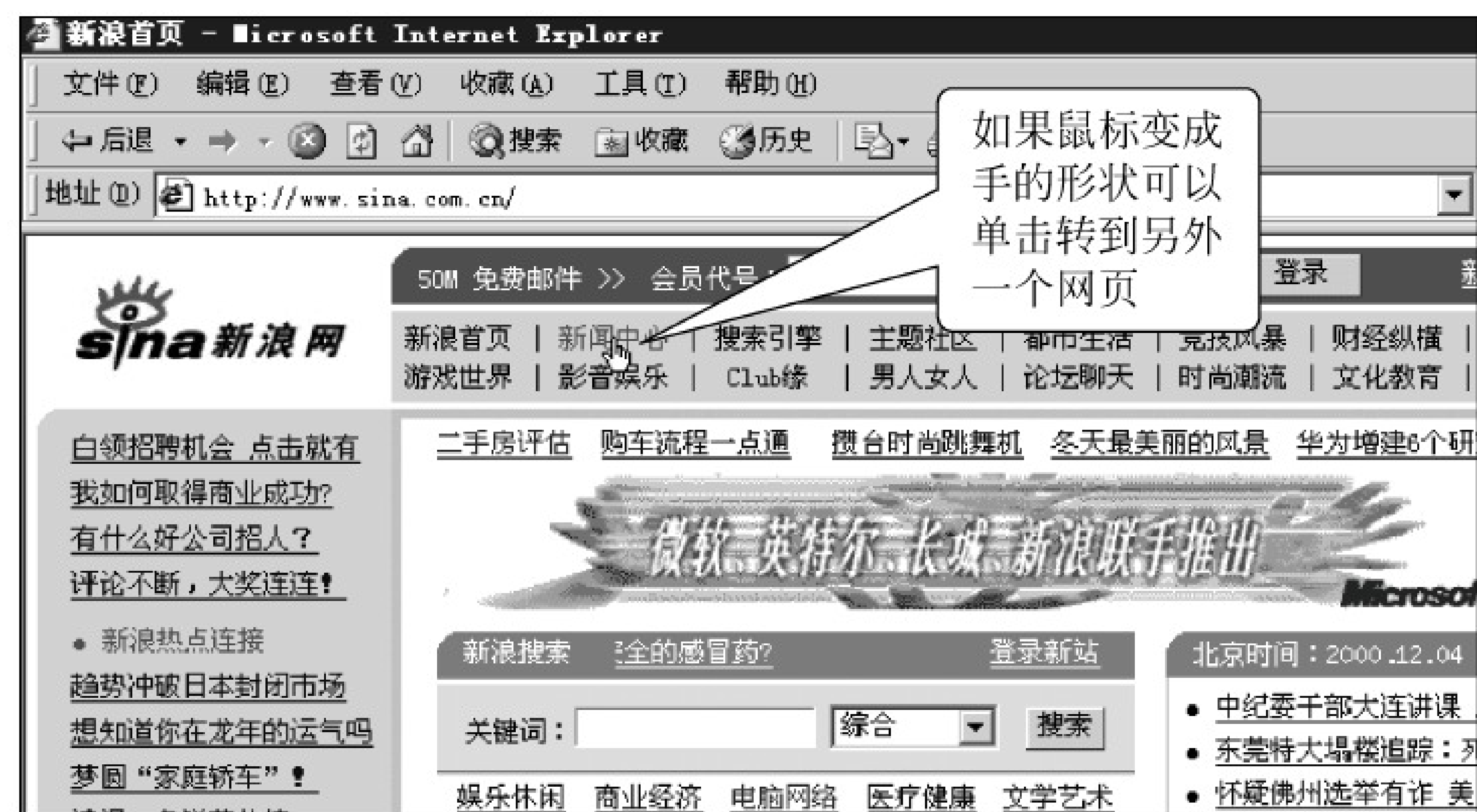


图 5-42　超链接的使用

(3) 保存网页中的信息

当浏览到某个自己感兴趣或者有意义的信息时，有必要将这些信息保存下来。在 Internet Explorer 中保存信息有几种类型：一种是保存整个网页；另一种是保存网页中的文本信息；还有一种是保存网页中的图片、动画、信息等；再有一种是保存网页中的超链接。保存网页中的信息，执行菜单命令“文件”→“另存为”，弹出如图 5-43 所示的“保存 Web”对话框。



图 5-43　网页“保存 Web”对话框

在对话框中选择保存网页的目录以及保存的文件名，然后单击“保存”按钮就完成了网页的保存。在保存时还可以在“保存类型”下拉框中选择将该网页保存成何种类型。

网页，全部(*.htm，*.html)——使用这种类型，可以将网页中所有的信息，包括文字、图片、动画等全部保存起来，除了将网页保存之外，还会自动保存一个与网页同名的文件夹，其中保存了该网页的所有图片或动画等。

Web 文档，单一文件(*.htm)——使用这种类型，可以保存网页中所有的信息，但是不会产生同名的文件夹。

网页，仅 HTML(*.mht)——使用这种类型，可以保存网页中的所有文字信息，但不会保存图片、动画等信息。

文本文件(＊.txt)——使用这种类型,将会把网页中的文字信息保存成一个没有任何格式的扩展名为.txt 的纯文本文件。

要保存网页中部分文本信息,可以先选择要保存的内容,右击鼠标,选择快捷菜单中的“复制”命令。然后打开文字编辑器,选择“粘贴”命令。完成网页的文本信息的保存。

要保存网页的图片信息,选择图片后,右击鼠标,选择快捷菜单中的“图片另存为”,输入要保存的目录和文件名,单击“保存”按钮即可。

要保存超链接,用鼠标右击要保存的超链接,从快捷菜单中,选择“目标另存为”,弹出如图 5-43 所示的对话框,选择保存链接的目录和名称,单击“保存”按钮,则可以保存链接所指的页面或文件。

(4) Internet Explorer 的使用技巧

① 设置浏览器的起始页

起始页是指 Internet Explorer 启动时显示的网页,如果用户每次上网都会首先浏览某个网页的话,就可以将这个网页设为起始页。

设置的方法如下:

执行菜单命令“工具”→“Internet 选项”,在 Internet 对话框中打开“常规”选项卡,在“主页”区域内的地址栏中(如图 5-44 所示)输入起始页的地址,然后单击“确定”按钮。这样每次打开 Internet Explorer 后就会自动访问并显示这个网页。



图 5-44　设置主页

② 加速浏览

现在的 Web 网页上有很多图片、广告动画、漂浮的广告图标等,在浏览 Web 页时往往会等待很长的时间,为了缩短下载时间并节省费用,使用者可以做一些设置,关闭图片、动画等的自动下载功能。具体操作方法如下。

执行菜单命令“工具”→“Internet 选项”,在 Internet 选项对话框中打开“高级”选项卡(如图 5-45 所示)。在“多媒体”区域,将“播放网页中的动画”、“播放网页中的声音”、“播放网页中的视频”、“显示图片”等选项取消。这样当浏览某个网页时,这些信息不会自动下载,进而提高了浏览的速度。

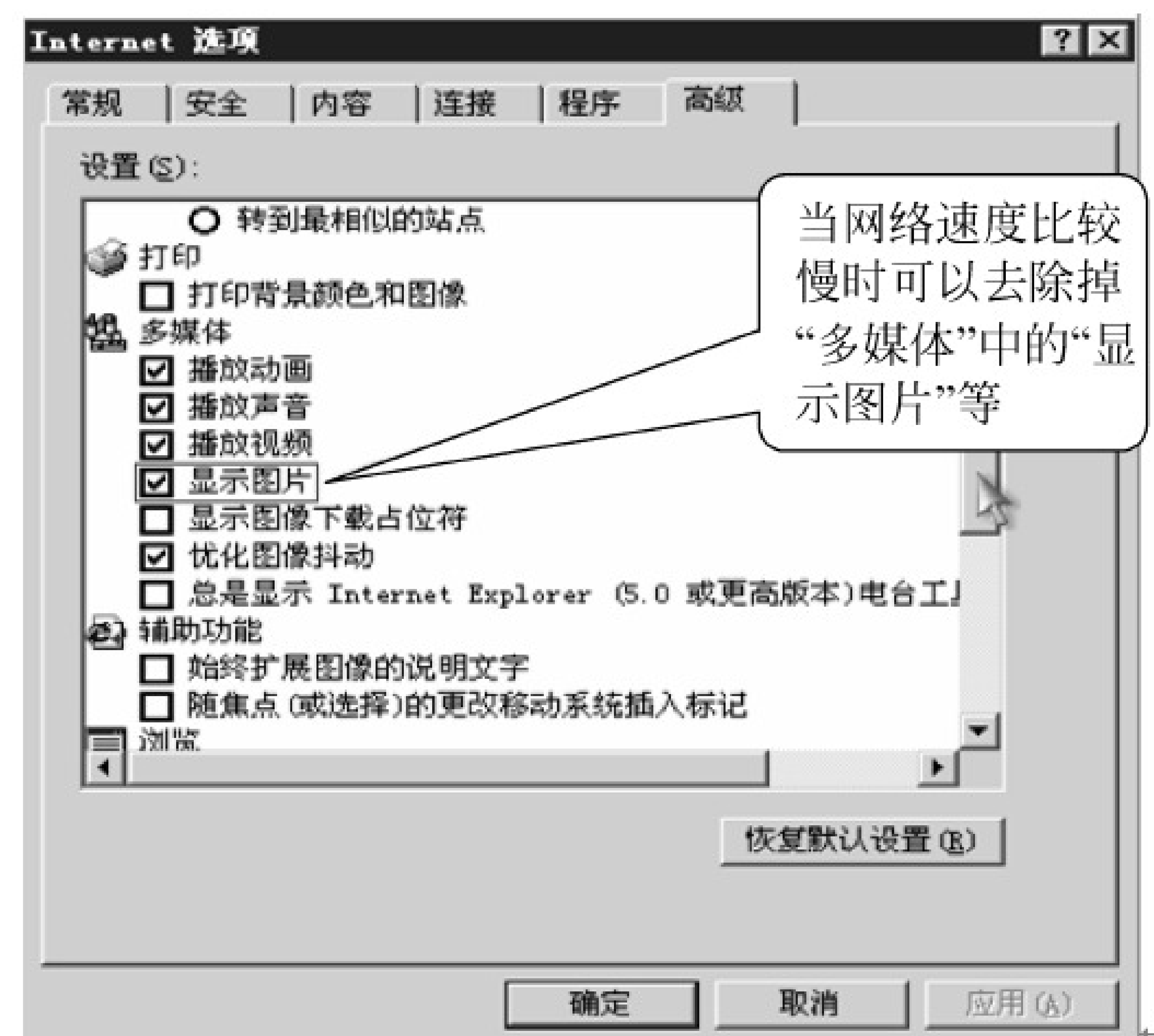


图 5-45　加速网页浏览

③ 解决乱码

在浏览某些网页时会出现一些奇怪的字符,这些字符称为“乱码”。这是因为世界各国的语言不同,这些语言在计算机中的编码也不同。例如,同样都是中文,内地是“简体中文”编码,而中国香港和台湾地区用的就是“繁体中文”编码。有时候IE会自动解决这个编码转换问题,但有时候却需要人工设置语言编码转换。人工设置操作方法如下。

执行菜单命令“查看”→“编码”命令(如图5-46所示)。在编码子菜单下列出了多种不同语言的编码,只要知道是哪个国家的网站,就可以在编码子菜单中选择相应的语言,即可解决乱码问题。也可以在编码子菜单中选择“自动选择”命令让浏览器对各种编码进行自动识别。



图 5-46　安装语言

2. 信息搜索

由于 Internet 的普及与发展所引起的信息量的爆炸式的增长，网络使用者面对大量的纷繁复杂的信息，往往感到茫然，无所适从。如何在这个纷繁复杂的信息海洋中准确、及时有效地发现并获取有价值的信息，并不是一件容易的事情，这需要使因特网的用户首先了解因特网上有哪些信息资源，并掌握获取各种不同类型的信息资源的方法，并能够对获取的信息进行评价。

（1）常用信息的搜索方法

① 浏览

获得某个信息的地址后，在浏览器中输入该地址，即可访问到该信息。也可以通过网页中的链接，找到链接的目标。

② 通过搜索引擎来查找信息

搜索引擎是在 Internet 中执行信息搜索的专门站点，它在 Internet 中主动搜索 Web 服务器中的信息，然后将搜到的信息建立索引，并将索引内容存储到可供查询的大型数据库中。当用户输入关键词查询时，它会告诉用户包含该关键词信息的所有网站或网页地址，并提供到网址或网页的链接。搜索引擎定期在 Internet 中漫游，搜索新的知识信息，并更新自己的索引数据库。用户可以利用搜索引擎所提供的分类目录和关键词搜索查找所需要的信息。

③ 信息搜索的策略

选择能够提供相关信息的优秀的搜索引擎。

了解各种搜索引擎所提供的信息的粒度和信息量。如果信息的粒度太粗，信息量过少，会让搜索者无法得到满意的信息内容；而信息粒度太细，信息量过大，搜索的结果冗杂繁复，又会让搜索者花费过多的时间进行进一步的信息筛选。

了解并掌握多种搜索引擎的搜索命令及搜索方法，便于熟练地使用。

有人说，会搜索才叫会上网，搜索引擎在网络冲浪中的地位是举足轻重的。

④ 搜索引擎的基本工作原理

搜索引擎有两种基本类型：全文搜索引擎和分类目录搜索引擎。

全文搜索引擎使用一个叫“网络机器人（Robot）”或叫“网络蜘蛛（Spider）”的软件，通过网络上的各种链接自动获取大量网页信息内容，并按一定的规则分析整理生成一个数据库。使用全文搜索引擎来搜索信息，也就是在数据库中查询相关的记录。Google、百度都是比较典型的全文搜索引擎系统。

分类目录搜索引擎则是通过人工的方式搜集整理网站资料形成数据库的。雅虎中国、搜狐、新浪等，包括网上的导航站点都属于分类目录。

搜索引擎的工作包括以下三个过程：

a）在 Internet 中发现、搜集网页信息。

b）对信息进行提取和组织建立索引数据库。

c）由检索器根据用户输入的查询关键字，在索引数据库中快速检索出相关信息，对检索结果进行排序，并将结果返回给用户。

表 5-3 列出了常用的搜索网站。

表 5-3 常用搜索引擎

搜索引擎名称	网 址
Google	http://www.google.com
百度	http://www.baidu.com
北大天网	http://e.pku.edu.cn/
雅虎中国	http://cn.yahoo.com/
搜狐	http://www.sohu.com
新浪	http://www.sina.com.cn

搜索引擎可以帮助您在 Internet 上找到特定的信息,但它们同时也会返回大量无关的信息。如果您多使用一些下面介绍的技巧,将发现搜索引擎会花尽可能少的时间找到您需要的确切信息。

(2) 高级搜索技巧

① 按类别搜索

许多搜索引擎(如 Yahoo!)都显示类别,如计算机和 Internet、商业和经济。如果选择其中一个类别,然后再使用搜索引擎,用户将可以选择搜索整个 Internet 还是搜索当前类别。显然,在一个特定类别下进行搜索所耗费的时间较少,而且能够避免大量无关的 Web 站点。

② 使用具体的关键字

如果想要搜索以鸟为主题的 Web 站点,可以在搜索引擎中输入关键字 bird。但是,搜索引擎会因此返回大量无关信息,如谈论羽毛球的"小鸟球(birdie)"或烹饪 game birds 不同方法的 Web 站点。为了避免这种问题的出现,要使用更为具体的关键字,如 ornithology(鸟类学,动物学的一个分支)。所提供的关键字越具体,搜索引擎返回无关 Web 站点的可能性就越小。

③ 使用多个关键字

用户还可以通过使用多个关键字来缩小搜索范围。例如,如果想要搜索有关佛罗里达州迈阿密市的信息,则输入两个关键字 Miami 和 Florida。如果只输入其中一个关键字,搜索引擎就会返回诸如 Miami Dolphins 足球队或 Florida Marlins 棒球队的无关信息。一般而言,提供的关键字越多,搜索引擎返回的结果越精确。

④ 使用布尔运算符

许多搜索引擎都允许在搜索中使用两个不同的布尔运算符:AND 和 OR。如果用户想搜索所有同时包含单词 hot 和 dog 的 Web 站点,只需要在搜索引擎中输入如下关键字:hot and dog。搜索将返回以热狗(hot dog)为主题的 Web 站点,但还会返回一些奇怪的结果,如谈论如何在一个热天(hot day)让一只狗(dog)凉快下来的 Web 站点。

如果想要搜索所有包含单词 hot 或单词 dog 的 Web 站点,只需要输入下面的关键字:hot or dog。

搜索会返回与这两个单词有关的 Web 站点,这些 Web 站点的主题可能是热狗(hot dog)、狗,也可能是不同的空调在热天(hot day)使人凉爽、辣酱(hot chilli sauces)或狗粮等。

⑤ 留意搜索引擎返回的结果

搜索引擎返回的 Web 站点顺序可能会影响人们的访问，所以，为了增加 Web 站点的点击率，一些 Web 站点会付费给搜索引擎，以在相关 Web 站点列表中显示在靠前的位置。好的搜索引擎会鉴别 Web 站点的内容，并据此安排它们的顺序，但其他搜索引擎大概不会这么做。

此外，因为搜索引擎经常对最为常用的关键字进行搜索，所以许多 Web 站点在自己的网页中隐藏了同一关键字的多个副本。这使得搜索引擎不再去查找 Internet，以返回与关键字有关的更多信息。

正如读报纸、听收音机或看电视新闻一样，应留意所获得的信息的来源。搜索引擎能够帮我们找到信息，但无法验证信息的可靠性。因为任何人都可以在网上发布信息。

5.2.5　网络论坛与博客

1. BBS 概述

论坛又名 BBS，全称为 Bulletin Board System（电子公告板）或者 Bulletin Board Service（公告板服务）。是 Internet 上的一种电子信息服务系统。它提供一块公共电子白板，每个用户都可以在上面书写，可发布信息或提出看法。它是一种交互性强，内容丰富而及时的 Internet 电子信息服务系统。用户在 BBS 站点上可以获得各种信息服务，发布信息，进行讨论，聊天等。

BBS 起源于 20 世纪 80 年代初，最早的 BBS 只提供消息投递和阅读功能，使用者通常是些计算机爱好者。随后，系统允许用户之间分享软件、文件，进行实时网络对话，信件传输等。为了提供更好的服务，一些站点实行收费政策，但目前 Internet 上还是有无数免费的 BBS 站点。一般 BBS 站点地址以域名形式出现，这些站点可通过远程登录进行连接，更多的站点采用 WWW 的形式供用户使用。

最初的 BBS 是以个人计算机为基础，通过 Modem 和电话线路连接，访问人数也受到电话线路的限制，而以 Web 形式架设的 BBS，可以接受访问的人次几乎不受任何限制。目前，BBS 涉及的题材广泛，是张贴通知、会议消息、招聘求职、专题讨论、困难求助等内容的地方，在这里人人都可以张贴消息，人人都可以很方便地获取自己所需要的消息。BBS 就像是一个虚拟社区，一些志趣相同的人常常聚集在一起讨论和交流。BBS 已经是因特网上最受人们青睐的地方之一。

著名的 BBS 站有：

- 水木清华 BBS 站（http://bbs.tsinghua.edu.cn/）
- 成都理工 BBS 站（http://bbs.cdit.edu.cn/）
- 东北大学（白山黑水）BBS 站（http://bbs.neu.edu.cn/）
- 广州中山大学（逸仙时空站）BBS 站（http://bbs.zsu.edu.cn/）
- 大连理工大学碧海青天 BBS 站（http://bbs.dlut.edu.cn/）
- 上海交大 BBS 饮水思源站（http://bbs.sjtu.edu.cn/）
- 北京大学 BBS 站（http://bbs.pku.edu.cn/）

• 复旦大学日月光华站（http://bbs.fudan.edu.cn/）
• 哈尔滨工业大学紫丁香 BBS 站（http://bbs.hit.edu.cn/）
• 新浪网论坛（http://people.sina.com.cn/forum.html）
• 中国中小学教育网 K12(http://sq.k12.com.cn/discuz/)

2. BBS 的使用

下面以基于 Web 的 BBS 站点为例来说明 BBS 的使用方法。

(1) 如何登录 BBS 站

在 Web 浏览器的地址栏内输入 BBS 网址，按回车键即可连接到 BBS 站。例如 K12 网站(http://sq.k12.com.cn/discuz/)。如图 5-47 所示。



图 5-47　论坛列表

(2) 如何注册新用户

一般情况下，很多 BBS 站都要求用户进行注册，在获得合法的用户名、密码后，才可以在 BBS 站内发表文章(也称帖子)、回复文章等。例如，在图 5-47 中，单击“个人信息”菜单项，将出现如图 5-48 所示的界面。在“账号”栏内输入账号名，例如 chinaboyo，在“密码”栏内输入密码，例如 12345。然后再填入一些必要的信息后，就可以注册成功。



图 5-48　用户登录

(3) 选择并进入主题社区

在论坛列表中，单击主题论坛即可进入相应的 BBS 论坛。例如，如图 5-49 所示为在“论坛列表”中选择进入 K12 网站的“教育论坛”。



图 5-49　主题论坛区

（4）如何写帖子

在主题论坛中，单击“发表新文章”菜单项（或“写新帖子”），将会出现如图 5-50 所示的界面。在表单中输入主题（即文章的标题），在正文框中输入帖子的具体内容。然后单击下面的“发表文章”按钮，文章自动张贴到论坛中去。



图 5-50　写新帖子

（5）如何读帖子

在论坛内的文章列表中，用鼠标双击要阅读文章的“主题”，所选定的文章内容将显示出来，如图 5-51 所示。

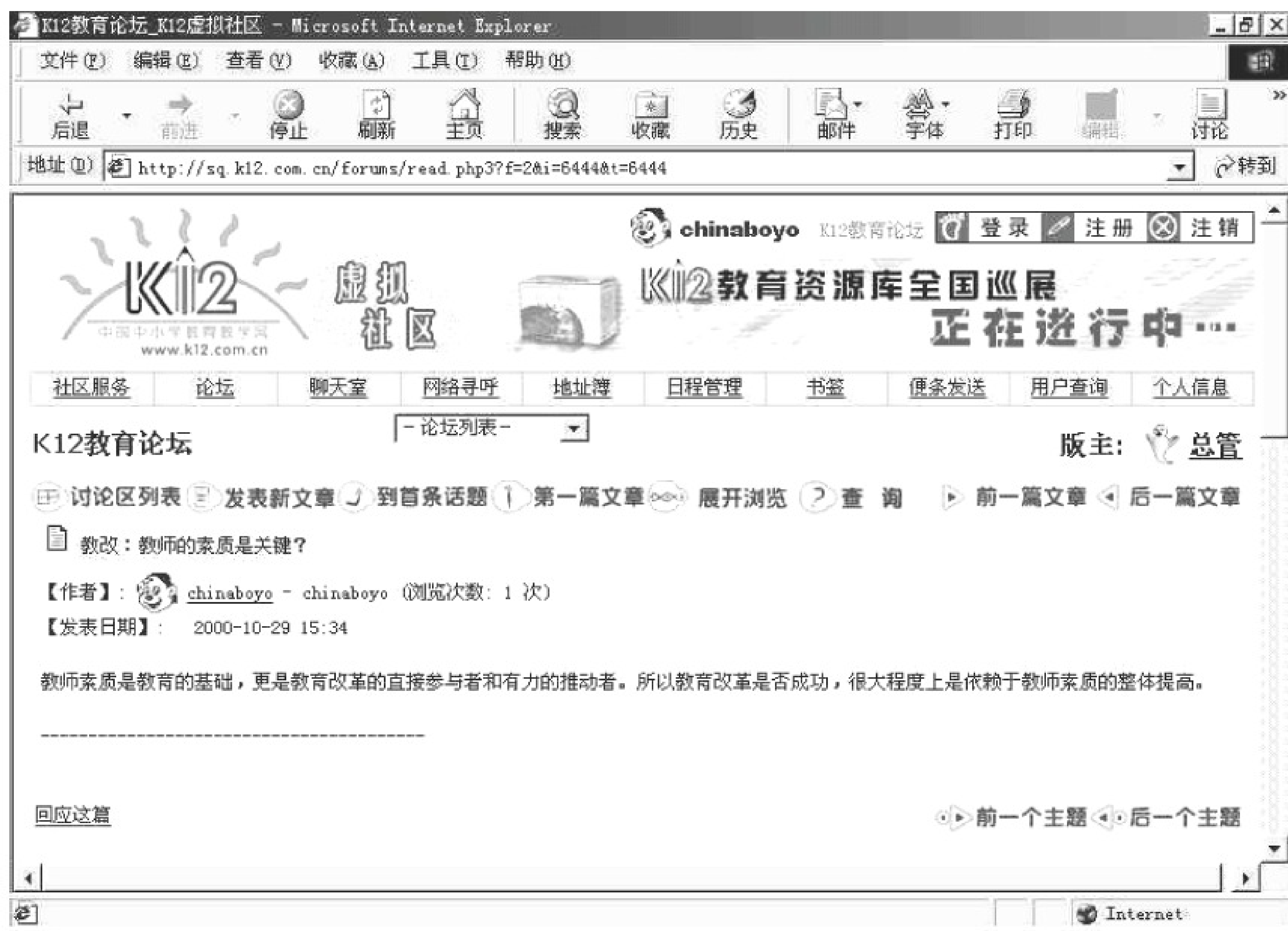


图 5-51　BBS 站的文章帖子

（6）回复帖子

如果要就所阅读过的文章内容写一个新帖子（即回复作者），只需用鼠标单击相应的文章回复功能项（例如图 5-51 中的“回应这篇”菜单项），将会出现回复界面。回复文章与前述的“写新帖子”的操作方法类似。

3. 博客概述

“博客”一词是由英文单词 Blog 翻译而来的。Blog 是 Weblog 的简称，而 Weblog 则是由 Web 和 Log 两个英文单词组合而成。Weblog 就是在网络上发布和阅读的流水记录，通常称为“网络日志”。简言之，Blog 就是以网络作为载体，简易迅速便捷地发布自己的心得，及时有效轻松地与他人进行交流，再集丰富多彩的个性化展示于一体的综合性平台。

不同的博客可能使用不同的编码，所以相互之间也不一定兼容。例如，百度空间使用的是 GB-2312 编码，新浪博客使用的是 UTF-8 编码。而且，目前很多博客都提供丰富多彩的模板等功能，这使得不同的博客各具特色。

（1）博客（Blog）在中国的发展历程

在网络上发表 Blog 的构想始于 1998 年，但到了 2000 年才开始真正流行。而 2000 年博客开始进入中国，并迅速发展，但都业绩平平。直到 2004 年木子美事件，才让中国民众了解到了博客，并运用博客。2005 年，国内各门户网站，如新浪、搜狐，原不看好博客业务，也加入博客阵营，开始进入博客春秋战国时代。起初，Bloggers 将其每天浏览网站的心得和意见记录下来，并予以公开，来给其他人参考和遵循。但随着 Blogging 快速扩张，

它的目的与最初已相去甚远。目前网络上数以千计的 Bloggers 发表和张贴 Blog 的目的有很大的差异。不过，由于沟通方式比电子邮件、讨论群组更简单和容易，Blog 已成为家庭、公司、部门和团队之间越来越盛行的沟通工具，因而它也逐渐被应用在企业内部网络（Intranet）。目前，BSP 商家风起云涌，已有数十家大型博客站点。目前，国内优秀的中文博客如表 5-4 所示。

表 5-4　国内优秀博客

博客大巴	新浪博客	网易博客	搜狐博客	Blog. cn
和讯博客	QQ 空间	天极博客	天涯博客	百度空间

（2）博客的分类

博客主要可以分为以下几大类。

① 基本的博客：Blog 中最简单的形式。单个的作者对于特定的话题提供相关的资源，发表简短的评论。这些话题几乎可以涉及人类的所有领域。

② 小组博客：基本的博客的简单变型，一些小组成员共同完成博客日志，有时候作者不仅能编辑自己的内容，还能够编辑别人的条目。这种形式的博客能够使得小组成员就一些共同的话题进行讨论，甚至可以共同协商完成同一个项目。

③ 亲朋之间的博客：这种类型博客的成员主要由亲属或朋友构成，他们是一种生活圈、一个家庭或一群项目小组的成员。

④ 协作式的博客：与小组博客相似，其主要目的是通过共同讨论使得参与者在某些方法或问题上达成一致，通常把协作式的博客定义为允许任何人参与、发表言论、讨论问题的博客日志。

⑤ 公共社区博客：公共出版在几年以前曾经流行过一段时间，但是因为没有持久有效的商业模型而销声匿迹了。廉价的博客与这种公共出版系统有着同样的目标，但是使用更方便，所花的代价更小，所以也更容易生存。

⑥ 商业、企业、广告型的博客：对于这种类型博客的管理类似于通常网站的 Web 广告管理。商业博客分为：CEO 博客、企业博客、产品博客、“领袖”博客等。以公关和营销传播为核心的博客应用已经被证明将是商业博客应用的主流。

（3）Blog 的使用

下面以畜牧人网站的博客为例来说明 Blog 的使用方法。

① 首先注册新博客，在图 5-52 中填好所有注册信息并输入正确的验证码。

图 5-52　博客注册页面

注意：*登录用户名必须用英文且简洁好记，因为注册以后所对应的域名是 http://bolg.xumuren.cn/u/登录名。可以轻松地记住这个网址。*

② 选择你喜欢的博客模板页面

在图 5-53 页面中，模板选择完毕就完成注册，可以在博客上发表文章了。



图 5-53 博客模板选择页面

③ 博客管理

在如图 5-54 所示的页面中,单击博客首页的“管理中心”按钮即可进入博客管理功能页面。



图 5-54 博客管理

④ 发表文章

在“日志管理”功能中,可以发表文章、备份文章、修改文章,如图 5-55 所示。



图 5-55 发表文章

⑤ 评论留言管理

可以管理每篇文章的所有评论以及留言,如图 5-56 所示。

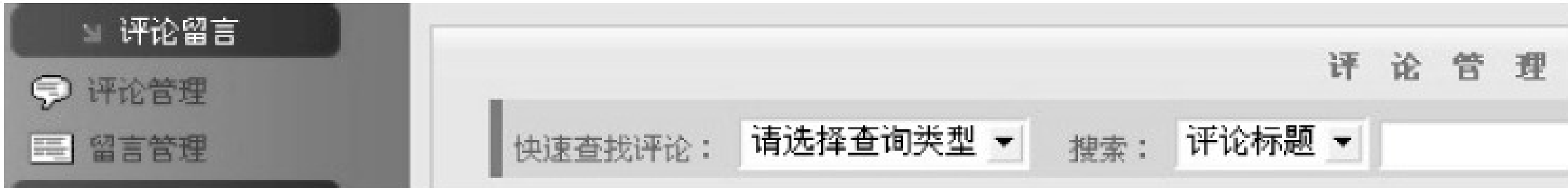


图 5-56 评论留言管理

⑥ 模板管理

可以更换模板，如果有兴趣的话，也可以自己修改模板，为自己打造一个有个性的博客页面(但以后更换模板的时候，如果没有备份模板的话，你的改动将不会被保存)，还可以将自己做的模板推荐出来供大家使用。如图 5-57 所示。

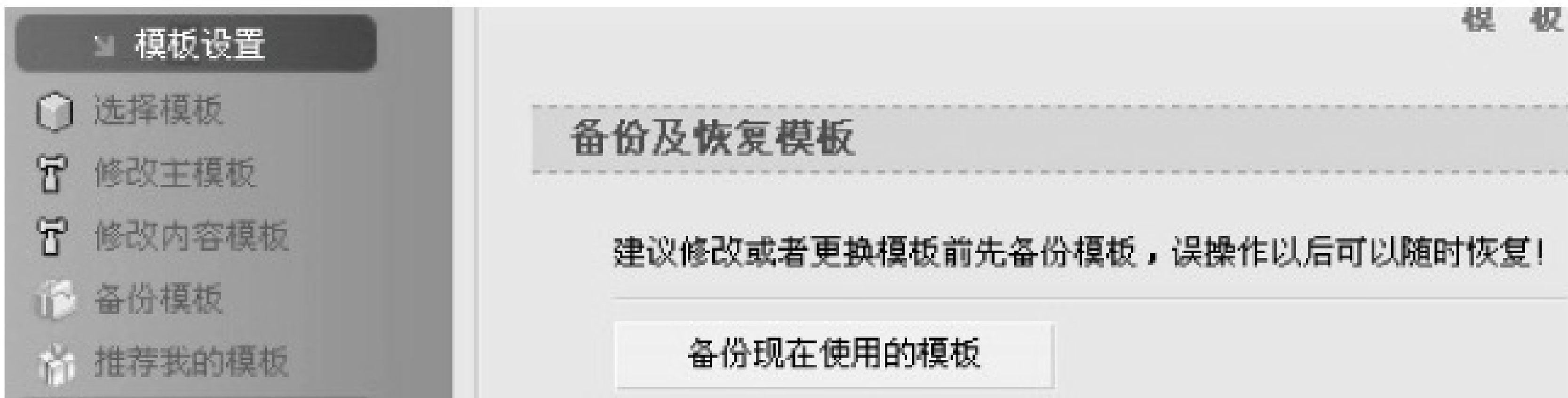


图 5-57　模板管理

⑦ 相册管理

可以上传照片，也可将上传的照片进行分类等操作，可以方便地找到所有照片，如图 5-58 所示。



图 5-58　相册管理

⑧ 文件管理

与相册管理类似，此功能可管理上传的所有文件和文档，如图 5-59 所示。



图 5-59　文件管理

⑨ 团队好友

博客可以让你认识很多好朋友，也可以通过这个功能将你的好朋友加入进来，甚至可以几个好朋友共同写一个博客，如图 5-60 所示。

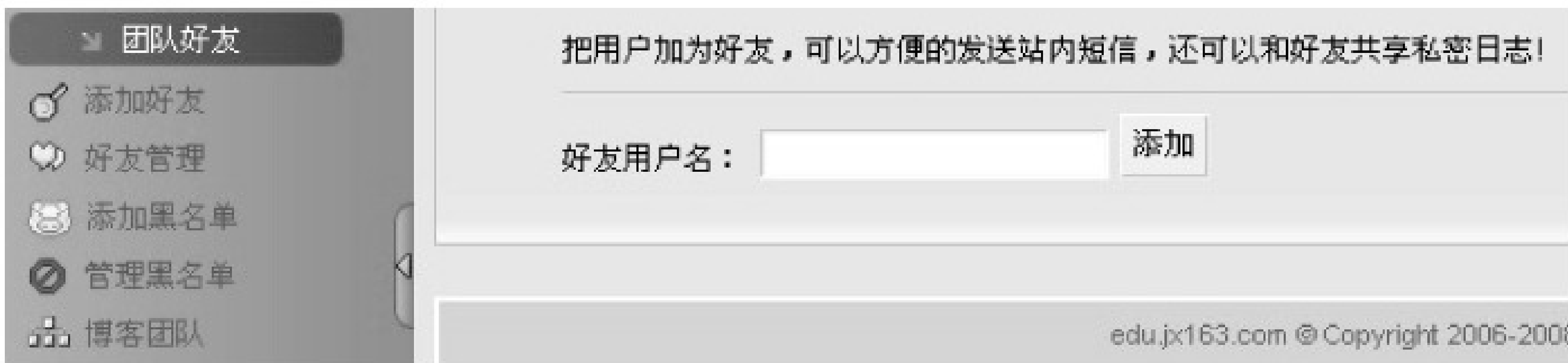


图 5-60　团队好友

⑩ 参数设置

使用此功能模块，可以修改你的博客的名字、每页显示的文章篇数、你的密码、你的公告、你的朋友的博客的连接。这是一个很有用的功能，也让你的博客与众不同，如图 5-61 所示。

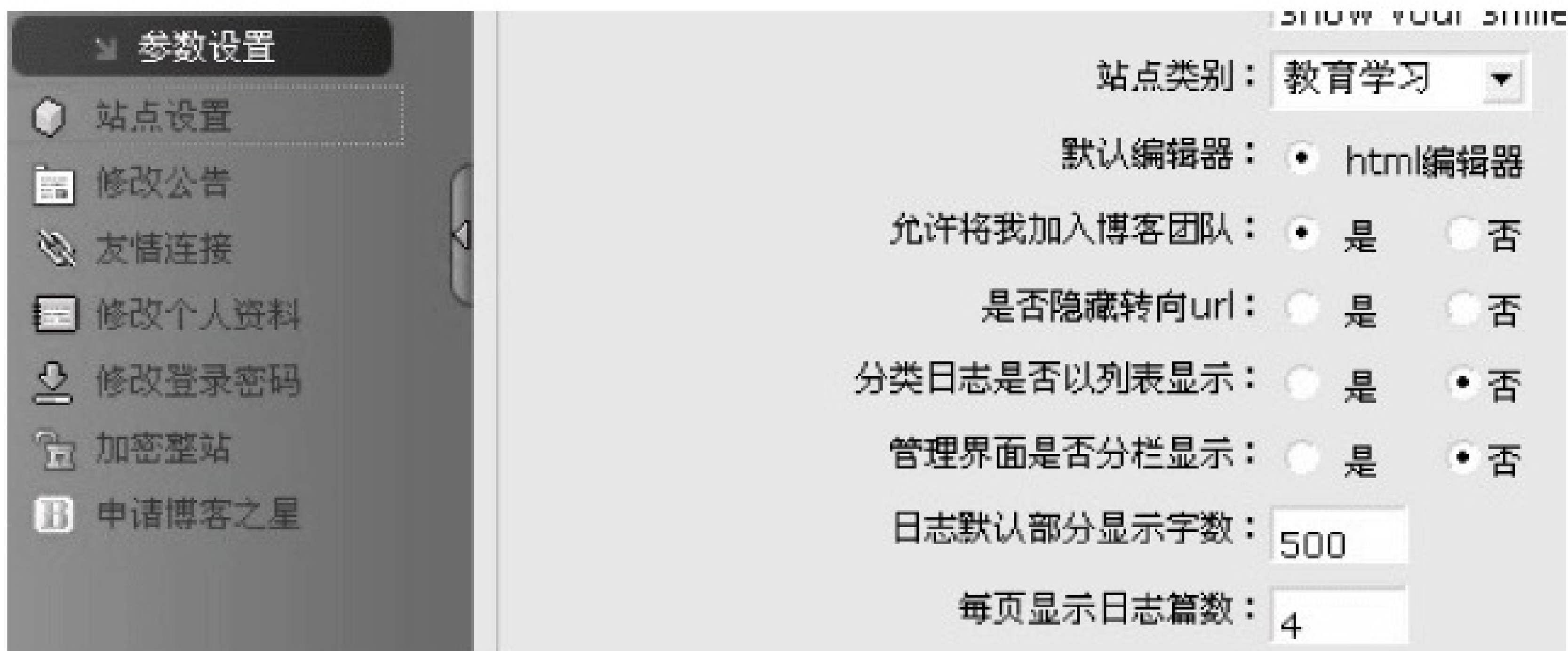


图 5-61　参数设置

5.2.6　网上即时通信

随着 Internet 技术的发展，出现了可以实现网上在线即时通信的技术与工具。利用这些工具，可以进行网上在线的实时交流，并可以实现传输文件等功能，这种交流方式通常被称做网上聊天。目前，Internet 上在线即时交流主要有两种形式。一种是基于 Web 页面的在线聊天室；另一种是使用各种专门的软件来实现实时交流。

1. 即时通信概述

即时通信(Instant Message，IM)是当今流行的一种以 Internet 网络及其他有线、无线网络为基础的实时通信方式。它通过通信系统建立网络虚拟社区，为用户提供实时有效的沟通手段。

当人们谈到 IM(即时通信)应用时，往往首先想到的就是聊天，但随着通信网与因特网的融合，即时通信软件作为一个崭新的个人信息交流平台正转向企业应用。IM 是现代交流方式的象征，也是迄今为止对人类社会生活改变最为深刻的一种网络新形态，企业使用 IM 能提高工作效率，节约费用。如企业员工之间交流工作，比用电话传递信息准确，并且省钱；生产商利用 IM 可以与伙伴和客户群保持密切联系；零售商可以用它进行客户服务。员工们可以通过 IM 的多方聊天功能召开在线会议；在 IM 会议室，某人可以加入或离开会议而不用担心影响其他人；随着会议进程的需要，可以随时邀请相关人员加入会议。这种 IM 在线会议不仅增加了工作效率，而且还会降低传统会议产生的种种成本。IM 的另一功能——在线感知，让 IM 用户的状态(比如在线、离线、离开座位等)可以显示在网络上。通过在线感知，员工可以实时获知其同事是否在线，从而方便下一步动作。这种面向个人的、用于朋友在线沟通的网络服务就和企业应用搭上了关系。

即时通信是一个终端服务，允许两人或多人使用网路即时地传递文字信息、档案、语音与视频。分手机即时通信和网站、视频即时通信，手机即时通信的代表是短信，网站、视频即时通信的如 QQ，MSN，擎旗 UcSTAR，百度 hi，恒聚 ICC 等应用形式。

任务实现：用户要使用 FTP 服务器上传和下载资料，必须会使用 FTP 客户端软件。这里主要介绍两种比较常见的软件，第一种为操作系统自带的 FTP 命令，通过 IE 资源管理器访问(此处通过命令提示符访问 FTP 服务器不做介绍)；第二种为使用专用的 leapFTP 软件。后一种能断点续传，传输数据比较稳定且完整。

2. 使用 IE 浏览器的方式

(1) 首先，打开 IE 浏览器，在地址栏处输入“ftp://192.168.1.4”，校外访问输入

“ftp://60.2.47.22”,然后按回车键登录。如果成功登录,则显示如图 5-62 所示的窗口。

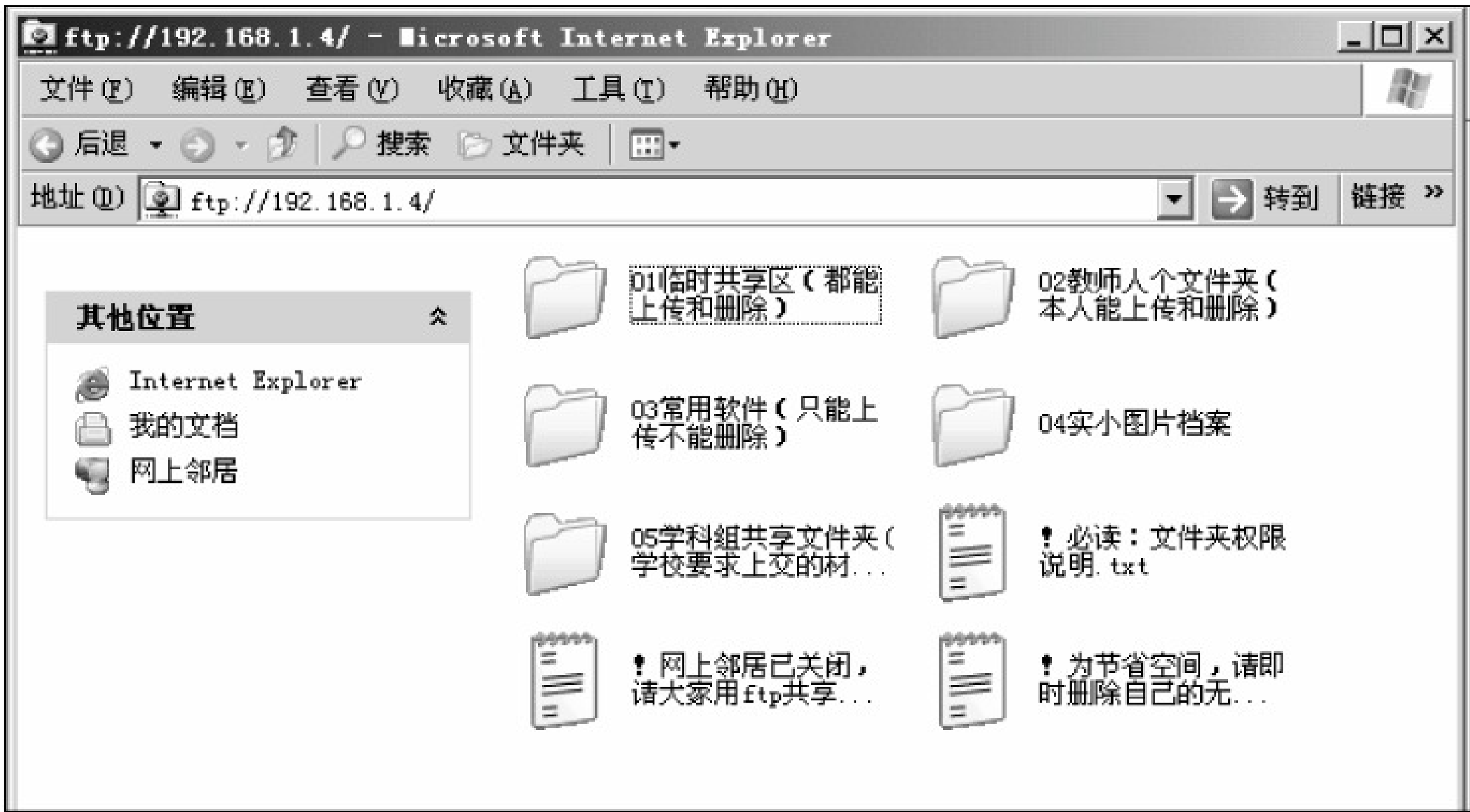


图 5-62　FTP 服务目录

(2) 在如图 5-62 所示的窗口空白处右击鼠标,在弹出的快捷菜单中选择“登录”项,如图 5-63 所示。弹出“登录身份”对话框,如图 5-64 所示。

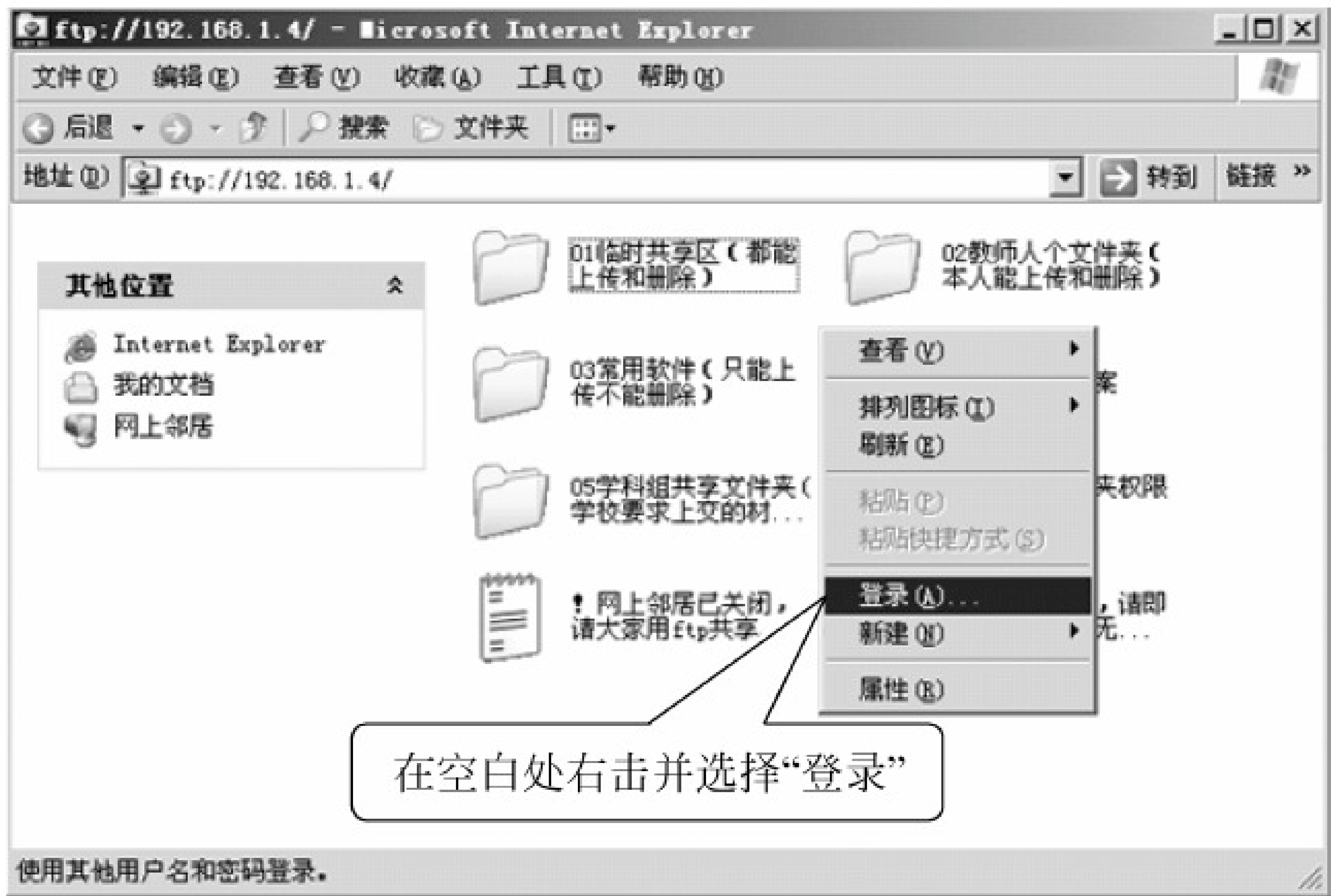


图 5-63　右击并选择“登录”

(3) 在“登录身份”对话框中输入用户名和密码,然后单击“登录”按钮。

(4) 现在用户进入到自己的 FTP 用户目录中,如图 5-65 所示。

现在就可以上传文件到 FTP 服务器中了。上传文件的方法与在“我的计算机”或“资源管理器”中复制文件是一样的。注意:选择文件时不要关掉 FTP 窗口,要最小化。具体操作步骤如下:

① 首先,打开计算机中存放文件的文件夹,选中要上传的文件,然后在其上右击,选择快捷菜单中的“复制”命令。

② 展开 FTP 窗口,在窗口空白处右击,选择快捷菜单中的“粘贴”项,即可将文件上传到服务器中。

注意:由于上传中文名字的文件夹会出错误提示,要单击“确定”按钮,文件夹就会传到服务器上,如图 5-66 所示。

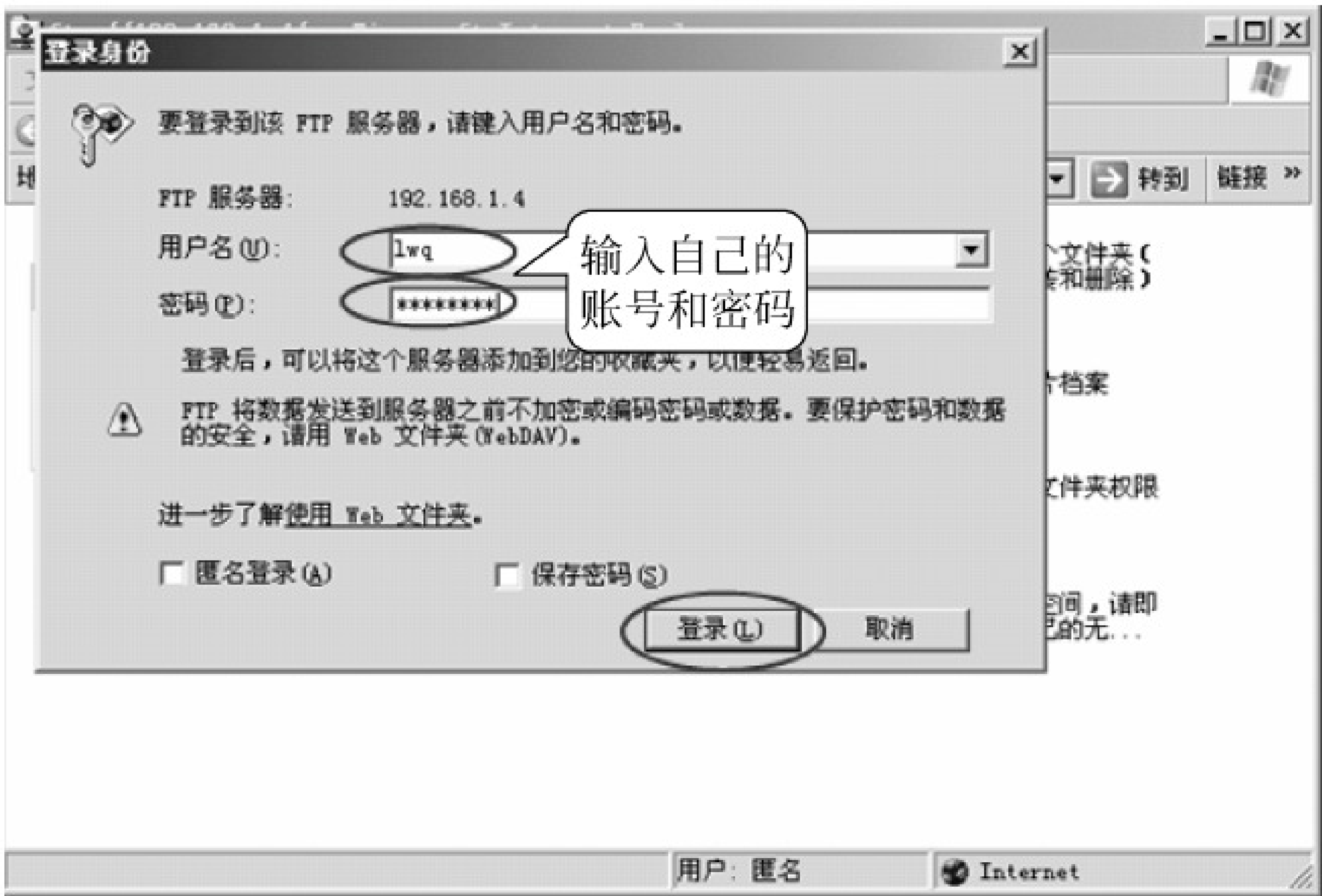


图 5-64　登录身份验证



图 5-65　登录成功窗口

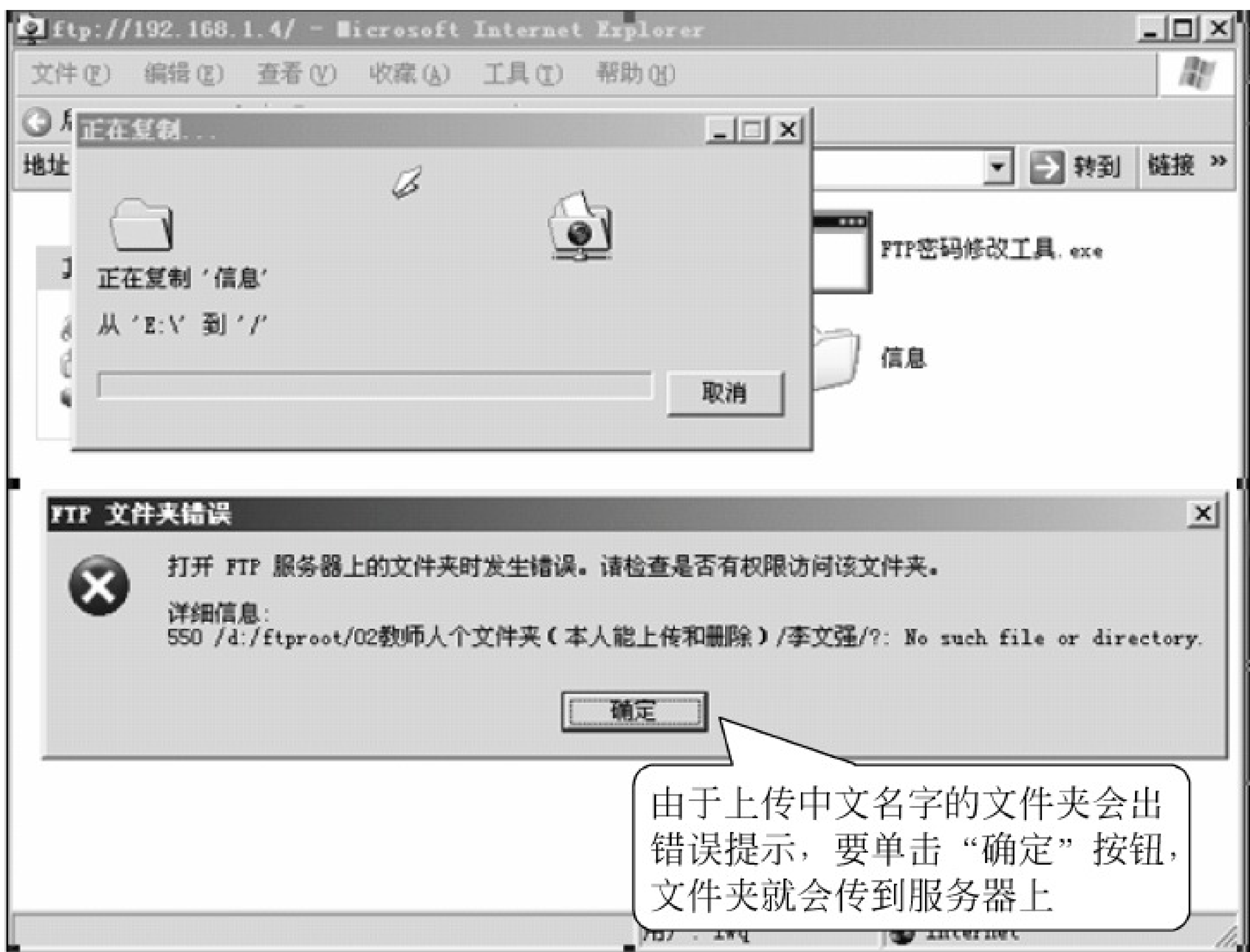


图 5-66　中文名导致报错

其他的操作(如下载文件、新建文件夹等)与资源管理器的使用方法一样,这里不再赘述。

3. 使用 FlashFXP 软件方式进行文件传输

使用 FlashFXP 软件方式进行文件传输具有支持断点续传、多线程上传等优点,尤其可以进行大文件的快速传输。

下载并安装 FlashFXP,双击打开桌面上的 FlashFXP 图标,运行程序。打开如图 5-67 所示的窗口。

(1) 执行菜单命令"站点"→"站点管理器",弹出"站点管理器"窗口。



图 5-67　"站点管理器"窗口

(2) 单击"新建站点"按钮,在"新建站点"对话框中输入站点名称,如图 5-68 所示。单击"确定"按钮。

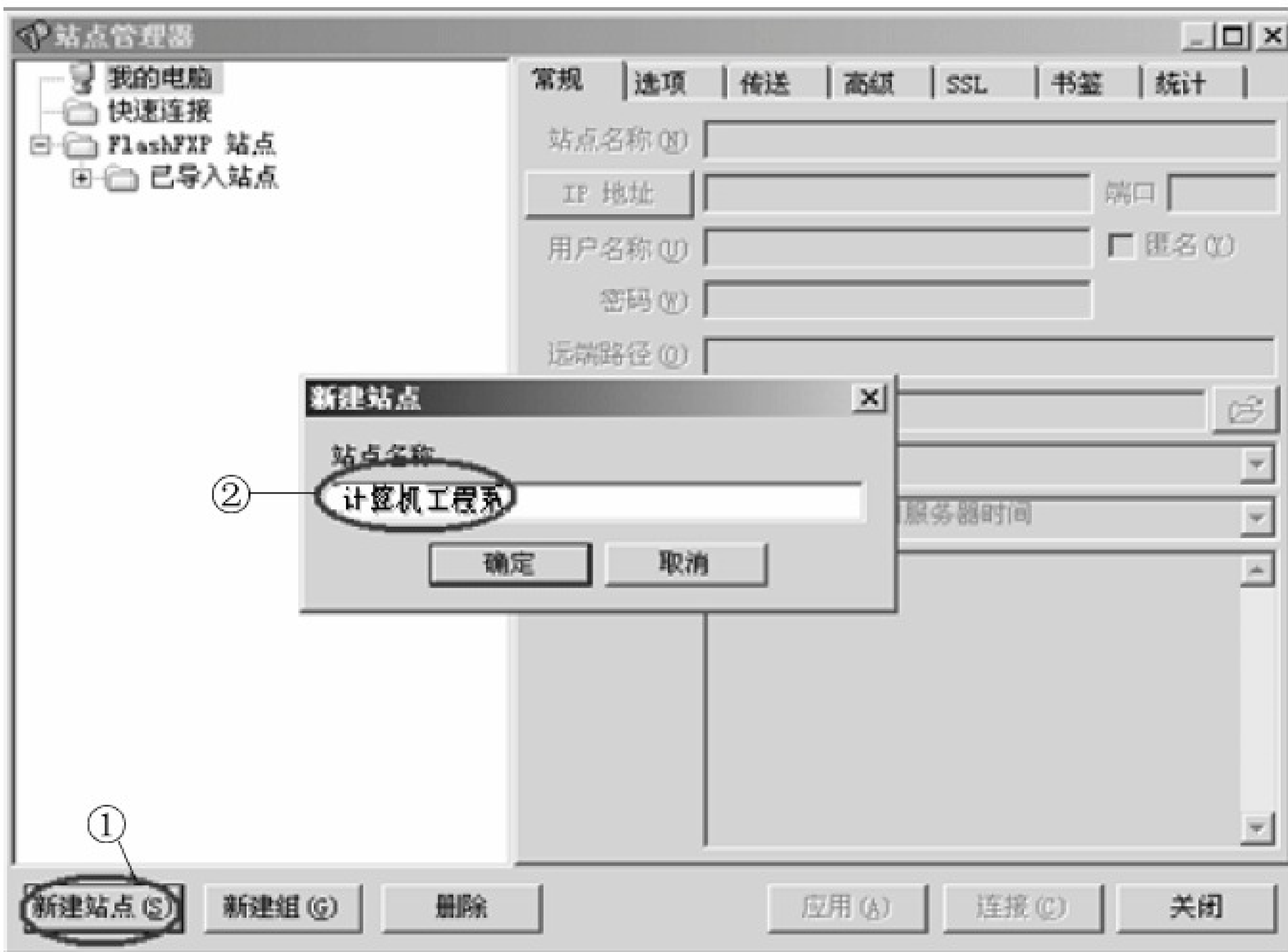


图 5-68　站点名称

(3) 在"站点管理器"窗口双击建立的站点,在窗口右侧,"常规"选项卡下输入用户名称、密码,IP 地址(校内用输入 192.168.1.4,校外用输入 60.2.47.22)等信息,单击"应

用”或“连接”按钮，如图 5-69 所示。



图 5-69　信息设置

（4）在 FlashFXP 窗口左右侧分别为“服务器上的文件”和“自己计算机中的文件”。进行文件上传、下载操作可以先选定对应的文件，用鼠标右击，如图 5-70 所示；也可以使用鼠标拖动文件或者使用工具栏按钮实现，如图 5-71 所示。



图 5-70　右键菜单

有了 FTP，无论我们身在何处，只要身边的计算机可以上网，就可来到学校 FTP 网站，把文件再下载下来。这样，资料就不用装在 U 盘中带来带去了，而且在家里也可以用，而且上传后的资料可以统一杀毒、统一备份，这就是 FTP 的最大好处。

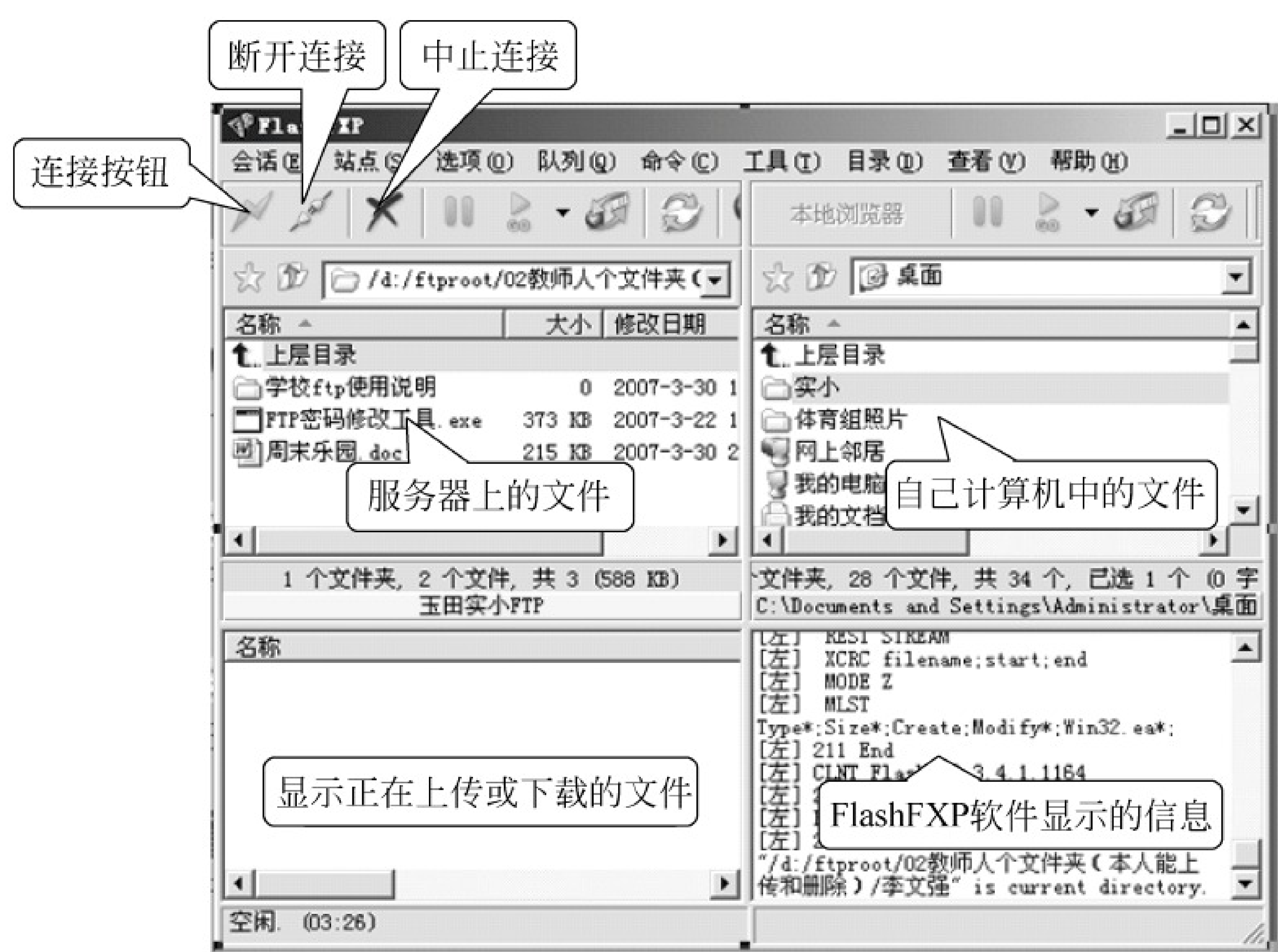


图 5-71　工具栏按钮

任务 5.3　家庭简易网络的组建

任务描述：目前家庭计算机越来越多，家庭接入互联网的需求也越来越大。本任务实现家庭计算机接入因特网。

5.3.1　接入因特网的方式

用户要使用 Internet 上的资源时，首先必须将自己的计算机接入 Internet，一旦用户的计算机接入 Internet，便成为 Internet 中的一员，可以访问 Internet 中提供的各类服务与丰富的信息资源。

1. ISP

ISP 是用户接入 Internet 的服务代理和用户访问 Internet 的入口点。所谓 ISP(Internet Service Provider)，就是 Internet 服务提供者，具体指为用户提供互联网接入服务、为用户定制基于互联网的信息发布平台以及提供基于物理层面上技术支持的服务商，包括一般意义上所说的网络接入服务商(Internet Access Provider，IAP)，网络平台服务商(Internet Platform Provider，IPP)和目录服务提供商(Internet Directory Provider，IDP)。各国和各地区都有自己的 ISP，在我国，具有国际出口路线的四大互联网运营机CHINANET、ChinaGBN、CERNet、CASNet 是全国最大的 ISP，它们在全国各地都设置了自己的 ISP 机构，如 ChinaNet 的 163 服务等。ISP 与互联网络相连的网络被称为接入网络，其管理单位称为接入单位。ISP 是用户和 Internet 之间的桥梁，它位于 Internet 的边缘，用户通过某种通信线路连接到 ISP，借助于 ISP 与 Internet 的连接通道便可以接入 Internet，如图 5-72 所示。

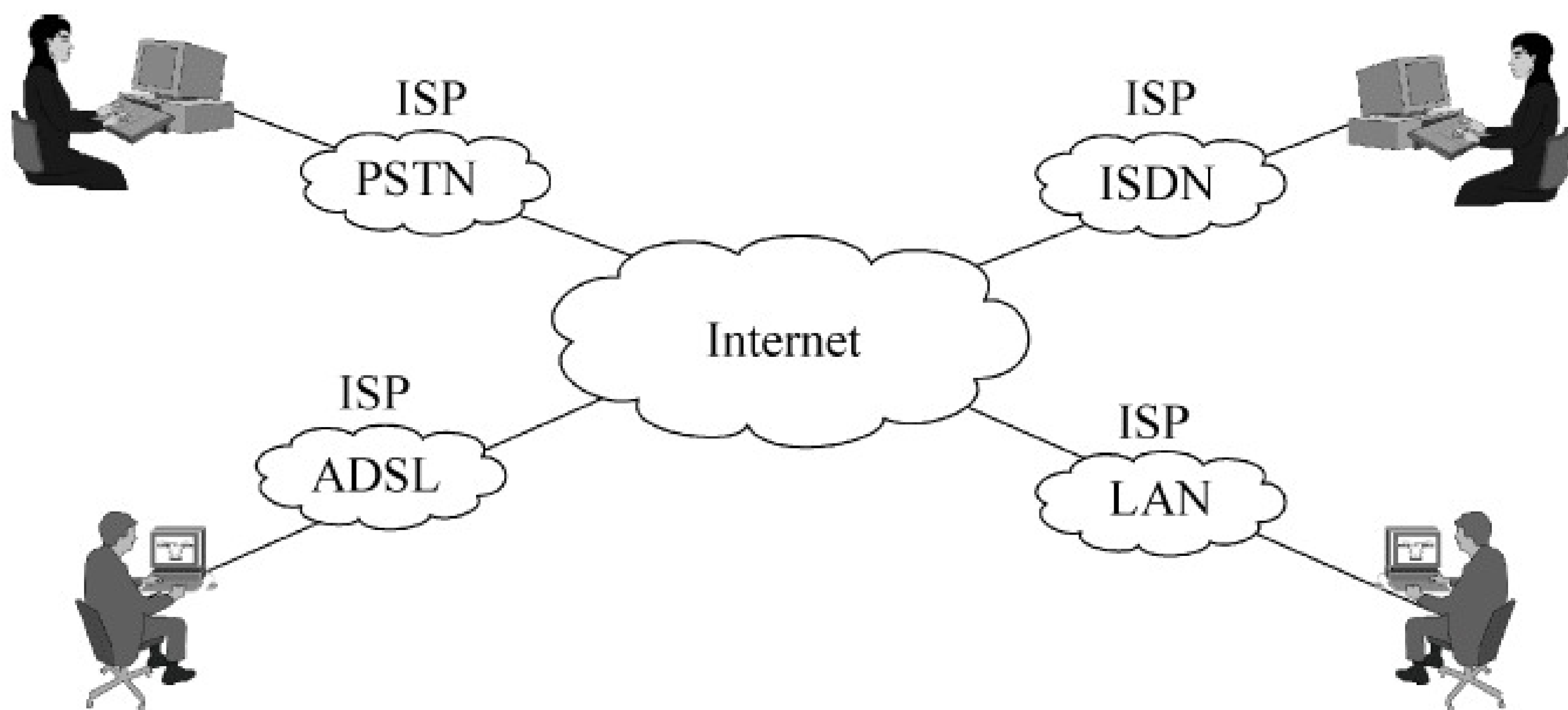


图 5-72　互联网示意图

至于用户能否有效地访问 Internet,则与 ISP 的选择直接有关。下面将介绍在选择 ISP 时应注意的几个问题。

(1) ISP 所在的位置

在选择 ISP 时,首先应考虑本地的 ISP,这样就可以减少通信线路的费用,得到更可靠的通信线路,花费更少的电话费用。比如通过电话线路(如首都在线)接入 Internet,如果选择的是本地的 ISP,费用按本地话费计算;否则按长途话费计算。

(2) ISP 的性能

① 可靠性:包括能否保证用户顺利地与之连接,在连接建立后能否保证连接不中断,能否提供可靠的电子邮件与域名服务器等服务。

② 传输速率:看看是否与国家或国际 Internet 主干连接,通常要选择一家规模比较大的 ISP,因为它可以支持比较高的传输速率。

③ 出口带宽:ISP 的所有用户共同分享 ISP 的 Internet 连接通道,如果 ISP 的出口带宽比较窄,它便可能成为用户访问 Internet 的“瓶颈”。

(3) ISP 的服务质量

对 ISP 服务质量的衡量是多方面的,如所能提供的增值服务、技术支撑、服务经验和收费标准等。增值服务是指为用户所提供的上网以外的一些服务,如根据用户需求定制安全策略、提供域名注册服务等。技术支撑除了一天 24 小时的连续运行外,还涉及能否为客户提供咨询或软件升级等服务。ISP 的服务经验与其经营理念、服务的历史长短及客户的情况等都有关。目前 ISP 常见的收费标准包括按传输的信息量收费、按与 ISP 建立连接的时间来收费或提供包月、包年的形式收费等。

2. 常见的 Internet 接入方式

在选择了合适的 ISP 以后,要解决的第二个问题是决定采用何种接入方式。网络接入方式的结构统称为网络接入技术。下面介绍最常用的家庭和企业接入技术。

(1) 公用电话交换网(PSTN)

PSTN(Published Switched Telephone Network)技术是利用 PSTN 通过调制解调器拨号实现用户接入的方式。这种接入方式是大家非常熟悉的一种接入方式,只需一个内置或外置 Modem,与 PC 相连或插入 PC,通过本地电话网 PSTN(程控电话交换网)接入 Internet,如图 5-73 所示。可以直接拨打 ISP 所提供的上网服务电话,如当地 163 或 169

电话接入 Internet。用户 PC 和 ISP 访问服务器之间的连接采用 PPP 协议实现，用户要使用支持 PPP 的通信软件来完成拨号主机与 ISP 服务器之间链路的建立、认证及网络层协议选择等过程，从而成为 Internet 的正式成员并访问 Internet 服务。

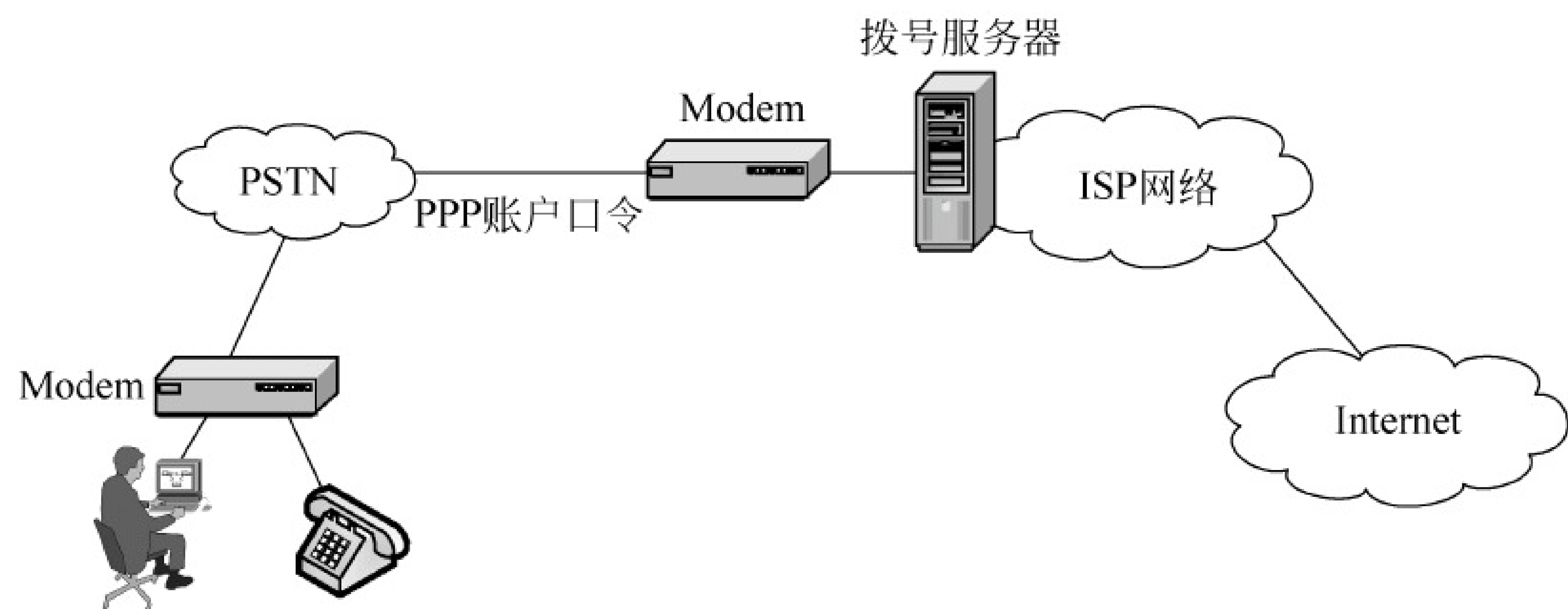


图 5-73　通过电话网连接到互联网

上网用户所需要的条件如下。

① 硬件需求

一台配有调制解调器(内置外置均可)的计算机，计算机的配置要求能运行 Windows 或其他的操作系统以及浏览器软件，一条电话线路(能拨打市话就可以)。

② 普通电话拨号用户主要参数配置

上网电话：拨打 169 或 163 均可接入 CHINANET 和 CNINFO。

③ 拨号上网域名服务器(DNS)和 IP 地址设置

在正常情况下，拨号上网用户不需要另行设置 IP 地址和 DNS，在拨号上网时系统会采用电信公司的拨号接入服务器自动分配的 DNS 和 IP 地址。

下面介绍电话拨号上网设置步骤(以 Windows XP 为例)。

拨号上网需要一根电话线和一个调制解调器，推荐使用 56kbps 调制解调器。所以首先安装调制解调器，以内置调制解调器为例。具体步骤如下。

① 断开电源，打开机箱安装内置调制解调器。

② 启动计算机，在 Windows XP 下安装调制解调器。执行“开始”→“设置”→“控制面板”命令，打开“控制面板”窗口。在窗口中双击“电话和调制解调器选项”图标，如图 5-74 所示。

打开“调制解调器”选项卡，单击“添加”按钮，出现如图 5-75 所示的界面。选取“不要检测我的调制解调器；我将从列表中选择(D)”复选框，然后单击“下一步”按钮。

③ Windows XP 会检测并辨认出用户使用的调制解调器，如图 5-76 所示，单击“选定的端口”单选按钮，选择端口，如“COM1”，单击“下一步”按钮。



图 5-74　“电话和调制解调器选项”界面

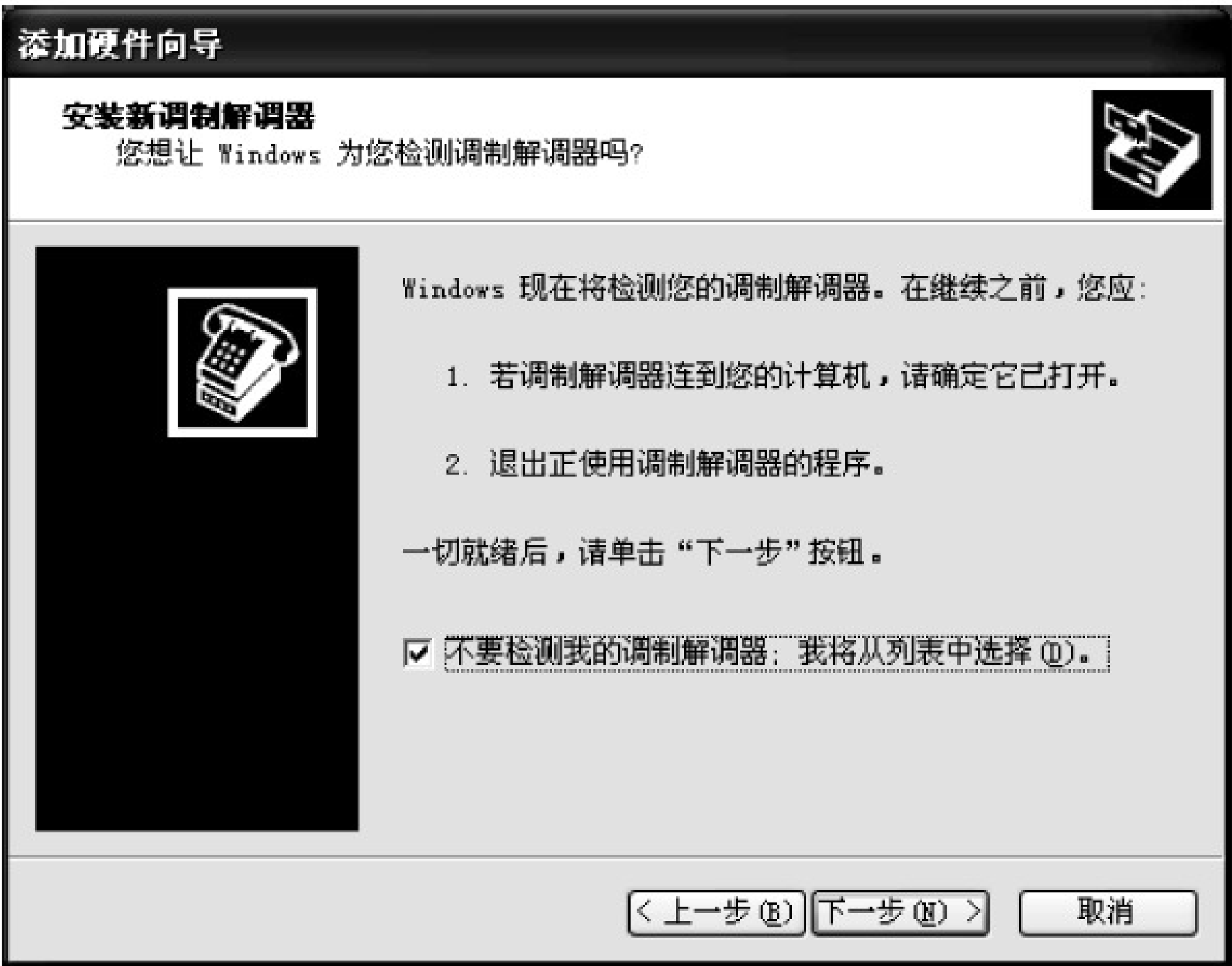


图 5-75　添加硬件向导



图 5-76　安装调制解调器

④ 系统进行驱动程序安装，安装完成后，单击“完成”按钮，如图 5-77 所示。

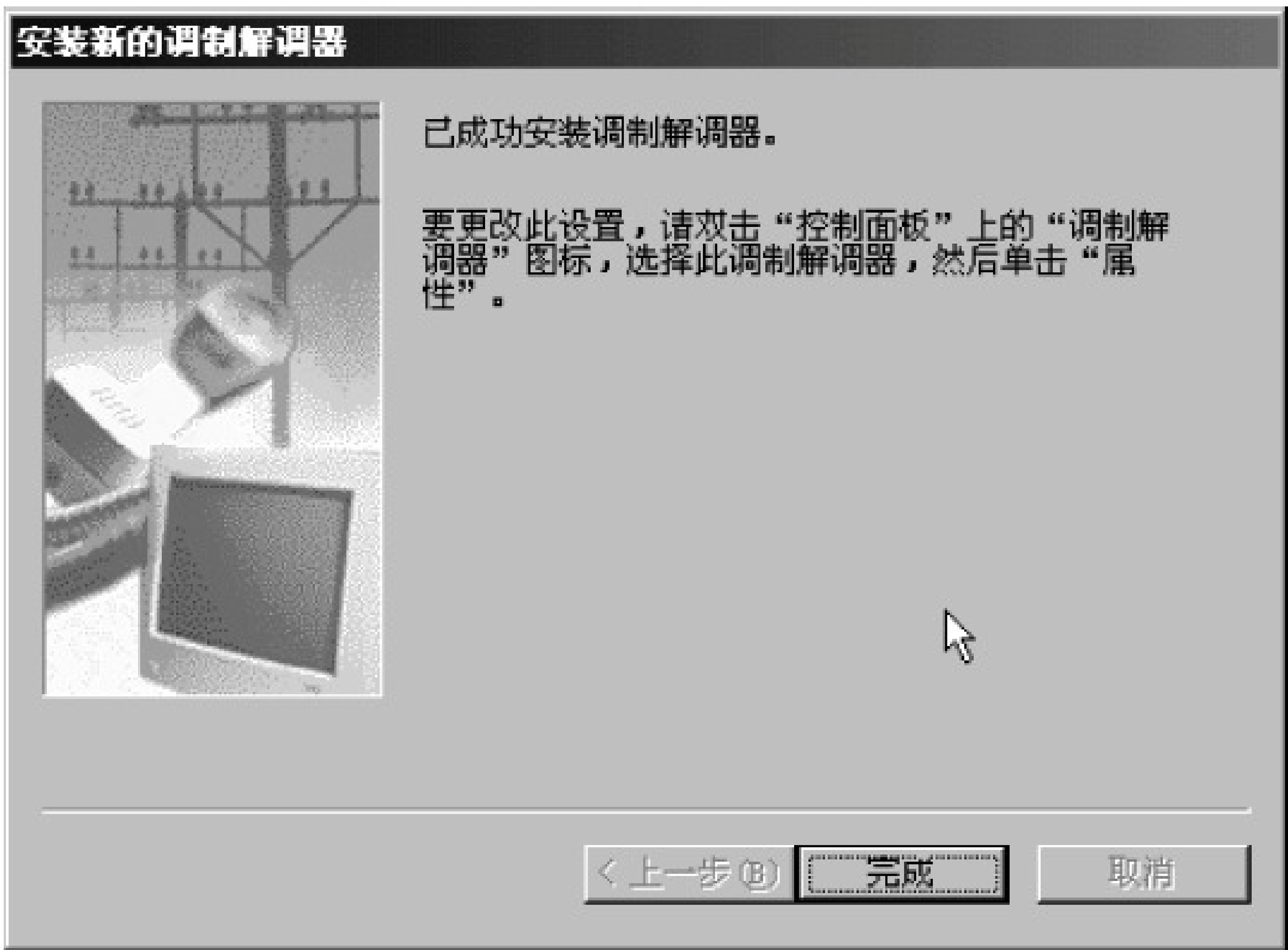


图 5-77　安装完成

⑤ 调制解调器的驱动程序安装成功后，可以对调制解调器的属性做一些相应的设置，包括占用的端口号、扬声器音量、传输速度和数据格式及呼叫的设置等，如图 5-78 所示。



图 5-78　调制解调器属性

⑥ 进行上网连接

安装好调制解调器后，要创建网络连接，该连接是一个拨号程序，使用它就可以和 ISP 建立信息通道，从而登录到 Internet。创建连接的方法如下。

在“控制面板”窗口，双击“网络连接”图标；执行菜单命令“文件”→“新建连接”；单击“下一步”按钮；选择“拨号到 Internet”单选项，单击“下一步”按钮；选择“手动设置”选项，单击“下一步”按钮；选择“通过电话线和调制解调器连接”选项，单击“下一步”按钮；在“区号”列表框中选择“中国(86)”选项，单击“下一步”按钮；填入用户名和密码，单击“下一步”按钮；单击“完成”按钮。

⑦ 进行拨号

双击“网络和拨号连接”窗口中的“连接到 163”图标，打开“连接到”对话框；在“用户名”文本框中输入用户在 ISP 申请的账户名，在“密码”文本框中输入用户密码，在“电话号码”文本框中输入对方服务器的电话号码；单击“连接”按钮，弹出连接状态的对话框，可以看到当前的拨号状态；当登录到网络后就可以看到“已创建连接”对话框，这表示用户已经成功地连入了 Internet；单击“关闭”按钮，关闭“已创建连接”对话框，在桌面任务栏右侧出现一个连接图标。

(2) xDSL 接入方式(Digital Subscriber Line，数字用户线路)

xDSL 是 DSL 的统称，即数字用户线路，是以铜电话线为传输介质的点对点传输技术。xDSL 是以铜质电话线为传输介质的传输技术的组合。xDSL 在每一条电路中都使用智能适配器，以便将现有的双绞线电缆分成两个信道：上行的信道和下行的信道。上行的信道将数据从用户送至电话公司的网络设备上，下行的信道将数据从电话公司的网络设备传送至用户。

除了使用已有的电缆设备和网络以外，xDSL 还具有可为用户带来高带宽的优势，下行传输速率可以达到 55Mbps，上行传输速率范围在 576kbps 到 1Mbps 之间。但 DSL 受距离的限制，它只能在短距离内提供业务，常见的数字用户专线有 ADSL、HDSL、VDSL 等。上行速率与下行速率不同的称为非对称的传送技术，并且通常上行速率要远小于下行速率。由于大部分 Internet 资源，特别是视频传输需要很大的下传带宽，而用户对上传带宽的需求不是很大，因此，“不对称”的 ADSL 和 VDSL 得到了大量的应用。

① ADSL

如图 5-79 所示是 ADSL 的宽带接入方式，它采用频分复用原理将数据信号和电话音频信号调制于各自频段，用户端设备 Modem 和局端设备 DSLAM 在这里主要完成数据调制解调和接口匹配功能，语音分离器则相当于一个低通滤波器，能够实现数据和话音信号的分

离,使两者互不干扰。对个人用户来说,只需在 PC 上装上网卡,在普通的现有的电话线上加装一台 ADSL Modem 即可上网,避免了电话拨号上网时不能使用电话的烦恼。目前,ADSL 所能提供的上行最高速率为 2Mbps,下行最高速率为 8Mbps。由于 ADSL 安装简单,不需重新布线就可享受高速的网络服务,因此为用户所接受。而 VDSL 可以提供更高速度的数据传输,短距离内的最大下传速率可达 55Mbps,上传速率可达 19.2Mbps,甚至更高。目前典型提供的是 10Mbps 上、下行对称速率,因而被视为 ADSL 的下一代,目前已开展这项业务。

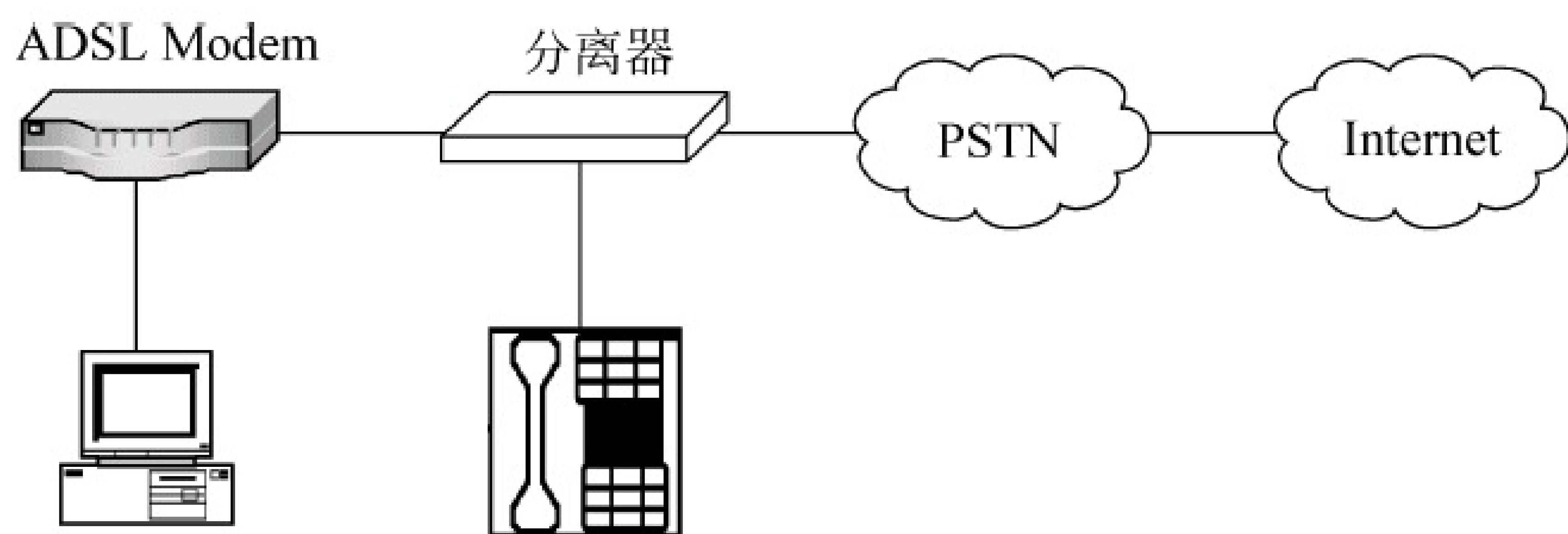


图 5-79 ADSL 联网示意图

ADSL 上网用户所需要的条件:一台能运行 Windows 或其他的操作系统以及浏览器软件的计算机和一部 ADSL 调制解调器。到电信局的电话线路不超过 5km,其他情况请咨询当地电信部门。

② 其他的 DSL

- HDSL:高速数字用户专线,优点是利用两条电话线进行数字数据的传输,采用对称技术,速率达到 1.544Mbps;缺点是传输距离短,最大传输距离仅为 12 000 英尺。
- SDSL:对称的数据用户专线,它提供上行传输速率和下行传输速率相同的 ADSL。SDSL 支持的上下行速率均为 384kbps。可以满足视频会议的要求。
- VDSL:超高速数字用户专线,是目前速度最快的 DSL 技术,只利用一条电话线,可提供 12～52Mbps 的下行带宽。传输距离为 10 000～60 000 英尺。
- RDSL:速度自适应用户专线,是一种能根据传送数据的网络的情况而自动调整速率的 ADSL。它可以根据传送信号的质量和信号传输的距离来调整速率。在一条线路上 RDSL 支持多种数字速率,并且可以迅速地适应这些不同的速率。

(3) 局域网接入

企业一般都是通过局域网接入 Internet 的,与普通个人用户的简单拨号上网不同,局域网接入 Internet 不能每台计算机都单独接入。有效地利用内部已经联网的优势,一方面共享接入线路资源;另一方面统一管理是选择局域网接入方案的重要着眼点。

目前用于中小规模局域网共享上网的软件大体分为两类:一类是代理服务器(Proxy Server)软件;另一类是宽带路由器。下面以宽带路由器接入方式为例来说明两种共享上网方法的实现。

① 硬件连接

- 建立局域网连接

用一根网线连接路由器和局域网中的交换机,如图 5-80 所示。也可以用一根网线将路由器与你的计算机网卡直接相连。

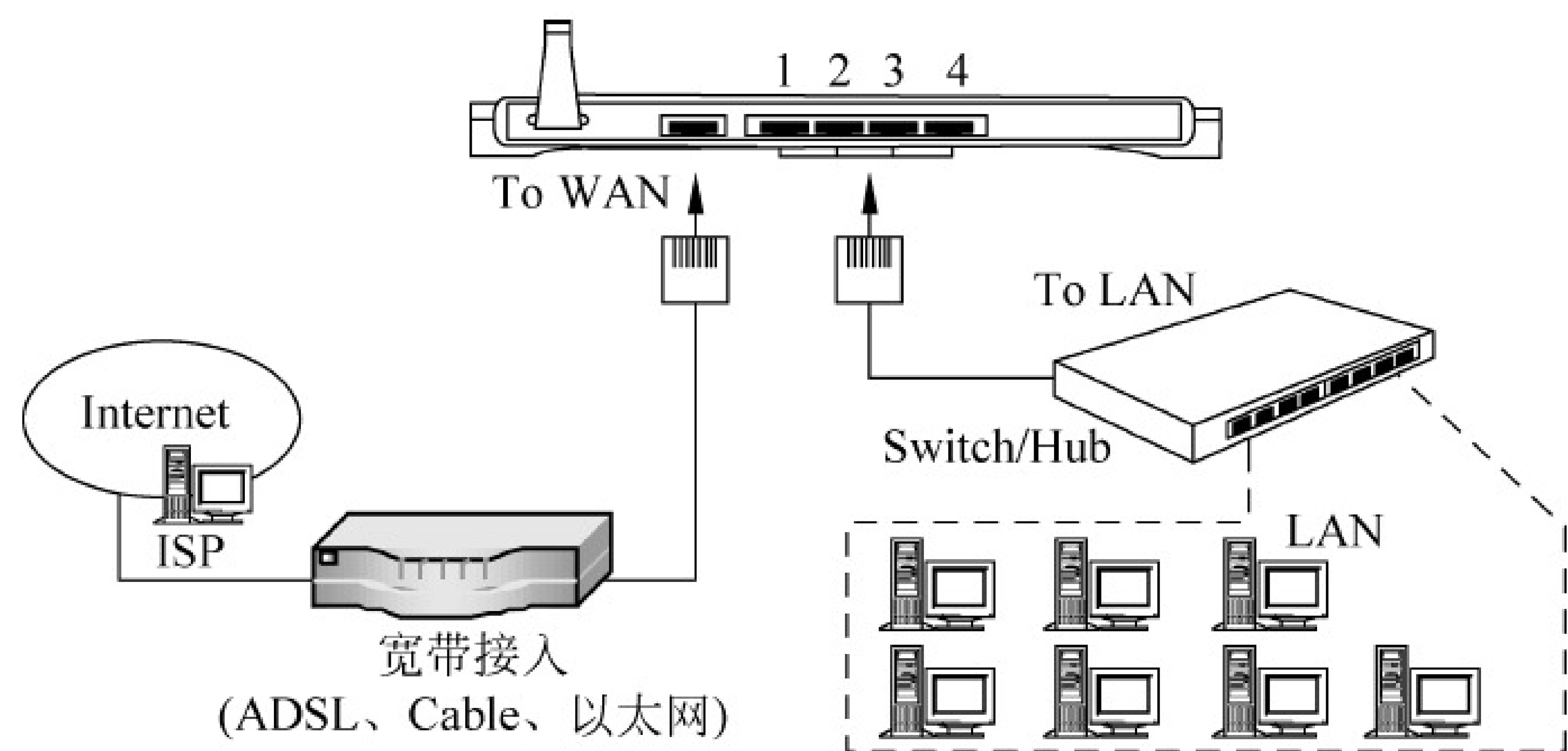


图 5-80　局域网接入示意图

• 建立广域网连接

用一根网线连接路由器和 ADSL Modem、Cable Modem 或以太网。

• 连接电源

将电源连接好，路由器将自行启动。

② 系统配置

• 进入路由器管理界面。一般宽带路由器的管理地址出厂默认为 IP 地址：192.168.1.1，子网掩码：255.255.255.0。用网线将路由器 LAN 口和计算机网卡连接好，因为路由器上的以太网口具有极性自动翻转功能，所以网线采用直连线或交叉线都可以，需要保证的是网线水晶头的制作牢靠稳固，水晶头铜片没有生锈等。

• 用鼠标右击桌面上的“网上邻居”，选择快捷菜单中的“属性”项，在弹出的窗口中双击“本地连接”图标，在弹出的窗口中单击“属性”按钮，在“此连接使用下列项目”栏选择“Internet 协议(TCP/IP)”双击，弹出“Internet 协议(TCP/IP)属性”对话框，如图 5-81 所示。在该对话框中选择“使用下面的 IP 地址”，然后在对应的位置填入下列信息。

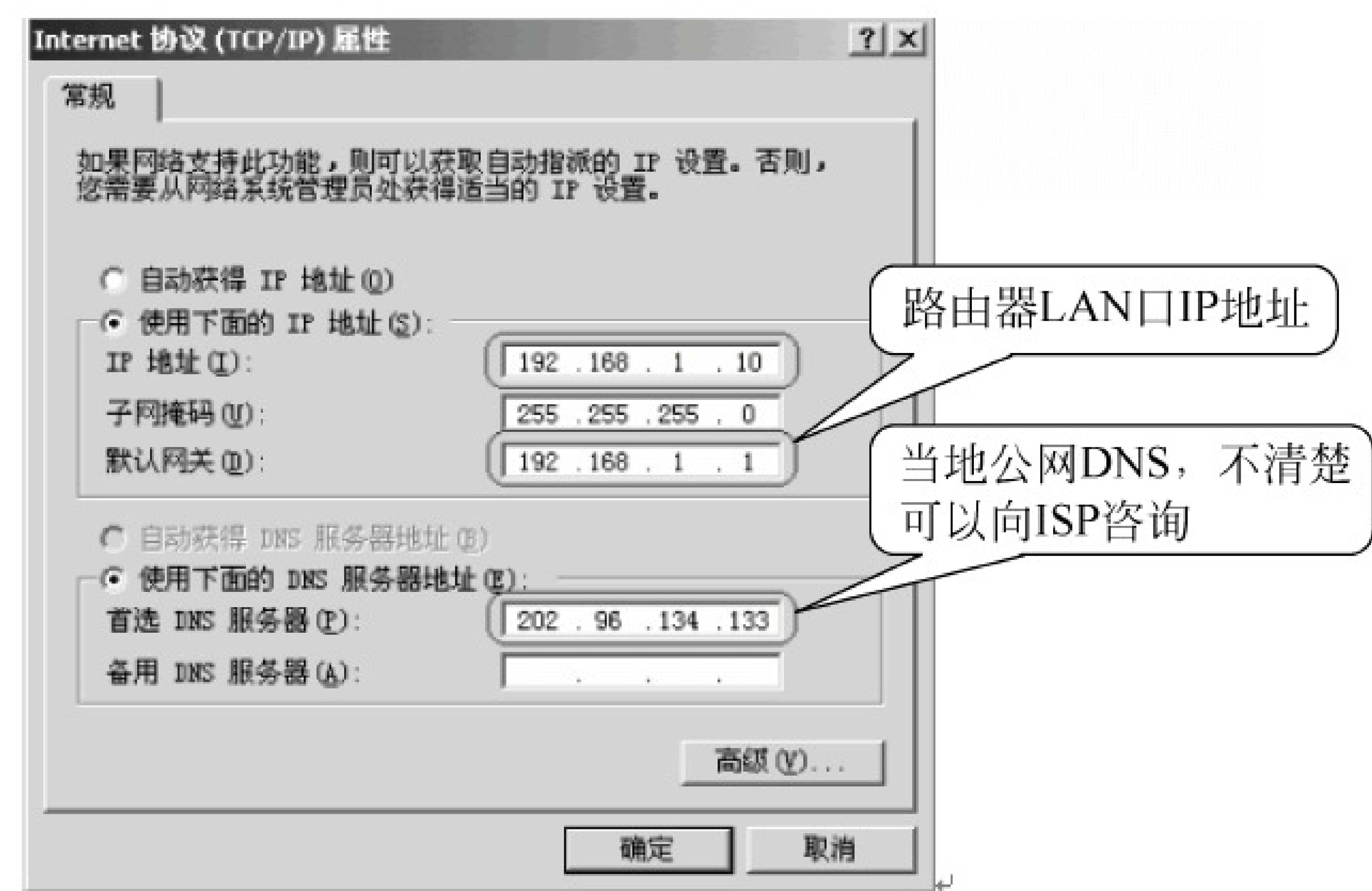


图 5-81　“Internet 协议(TCP/IP)属性”对话框

IP 地址：192.168.1.X(X 范围为 2～254)、子网掩码：255.255.255.0。

默认网关：192.168.1.1 等，输入完成后，单击“确定”按钮，直到退出即可。

- 打开 IE 浏览器，在地址栏输入“192.168.1.1”并按回车键，正常情况下会出现要求输入用户名和密码的对话框。用户名和密码一般默认都是 admin。
- 进入路由器管理界面，在左列执行菜单命令“网络参数”→“WAN 口设置”，配置路由器面向 Internet 方向的 WAN 口的工作模式；假设宽带接入方式为 ADSL→PPPoE，那就选择“WAN 口连接类型”为“PPPoE”，填入“上网账号”、“上网口令”，如果是包月用户，再选择连接模式为“自动连接”，单击“保存”按钮即完成配置。保存完后“上网口令”框内填入的密码会多出几位，这是路由器为了安全起见专门设置的。
- 然后单击管理界面左列的“运行状态”，在运行状态页面“WAN 口属性”栏，开始时看不到对应的 IP 地址子网掩码默认网关 DNS 服务器等地址，说明路由器正在拨号过程中，等到这些地址都出现了相应的信息后，将其中的 DNS 服务器地址填入计算机“Internet 协议(TCP/IP)属性”页面 对应位置确定后，基本的设置就完成了，没有大碍的话整个局域网就可以上网了。

5.3.2 广域网及其协议

1. 广域网

(1) 广域网基础

广域网(Wide Area Network，WAN)是在一个广泛的地理区域内建立的计算机通信网络，地理区域可以是一个城市，一个国家，甚至是全球。由电信运营商提供的设备作为信息传输平台。而在实际应用中，局域网(LAN)与广域网互联，且是作为广域网的一个终端系统。组建广域网必须按照一定的体系结构和网络协议进行，以实现不同系统的互联和相互协同工作。WAN 一般都是作为骨干网而设计的，而用户必须通过接入网与 WAN 相连，才能与远程用户之间通信。单个用户一般都是通过 Modem 拨号连接，而多个用户是在本地有 LAN，通过 LAN 接入与广域网连接。一般来讲，接入方式可以分为：HFC 接入、xDSL 接入、Modem 接入以及无线接入等。

对照 OSI 参考模型，广域网技术主要位于底层的三个层次，分别是物理层(Physical Layer)、数据链路层(Data Link Layer)和网络层(Network Layer)。

(2) 广域网连接类型

① 点对点链路

点对点链路(PPP)提供的是一条预先建立的从客户端经过运营商网络到达远端目标网络的广域网通信路径。一条 PPP 链路就是一条租用的专线，也就是说可以在数据收发双方之间通过广域网建立起永久性的固定连接。网络运营商负责对 PPP 链路的维护和管理。PPP 链路提供了两种数据传送方式：一种是数据报传送方式，其原理是将要传输的数据分割成一个个小的数据帧进行传送，其中每一个数据帧都带有自己的地址信息，到达信宿，也就是传输数据的目的地时需要对每一个数据帧进行地址校验；另外一种是数据流传送方式，该方式与数据报传送方式不同，用数据流取代一个个的数据帧作为数据发送单位，整个数据流具有一个地址信息，只需要进行一次地址验证即可。如图 5-82 所示的



图 5-82 跨广域网连接

就是一个典型的跨越广域网的点对点链路。

② 电路交换

电路交换是 WAN 所使用的一种交换方式。当收发双方要进行会话时，可以通过运营商网络为会话过程建立、维持和终止一条专用的物理链路。电路交换也可以提供数据报和数据流两种传送方式。电路交换在电信运营商的网络中被广泛使用，其操作过程与普通的电话拨叫过程非常相似。综合业务数字网（ISDN）就是一种采用电路交换技术的广域网技术。

③ 包交换

包交换也是 WAN 经常采用的一种交换技术，通过包交换，网络设备可以共享一条点对点链路，通过运营商网络在设备之间进行数据包的传递。包交换主要采用统计复用技术在多台设备之间实现电路共享。ATM、帧中继、SMDS 以及 X.25 等都是采用包交换技术的广域网技术。

④ 虚拟电路

虚拟电路是一种逻辑电路，可以在两台网络设备之间实现可靠通信。虚拟电路可以分为两种不同的形式，分别是交换虚拟电路 SVC（Switched Virtual Call）和永久性虚拟电路 PVC。交换虚拟电路（SVC）是按照需求动态建立的虚拟电路，其通信过程主要包括呼叫建立、数据传送、呼叫清除等几个过程。呼叫建立主要是在通信双方设备之间建立虚拟电路；数据传送阶段就是通过虚拟电路在设备之间传送数据；呼叫清除则是数据传送结束时，清除通信设备之前建立起来的虚拟电路。因为 SVC 的动态性，呼叫建立和呼叫清除都需要占用很多的网络带宽，所以 SVC 主要适用于非经常性的数据传送网络。但是相对于永久虚拟电路来说，SVC 是比较实用的。永久性虚拟电路（PVC）是一种永久性建立的虚拟电路，像专线一样，无需建立和清除连接，可以直接传送数据。因为这种固定性，不需要使用额外的带宽，PVC 可以应用于数据传送频繁的网络环境，所以对带宽的利用率更高，不过成本较高。无论是交换虚拟电路还是永久虚拟电路，都是几条“虚拟电路”链路共享一条真正的物理链路。换句话说，通信设备之间至少有一条物理链路，几条虚拟电路都可以在这条物理链路上传输数据。

（3）广域网基本设备

在广域网环境中可以使用多种不同的网络设备。下面就着重介绍一些比较常用的广域网设备。

① 广域网交换机

广域网交换机（WAN Switch）是在运营商网络中使用的多端口网络互联设备。广域网交换机工作在 OSI 参考模型的数据链路层，可以对帧中继、X.25 以及 SMDS 等数据流进行操作。如图 5-83 所示是位于广域网两端的两台路由器通过广域网交换机进行连接的示意图。

② 接入服务器

接入服务器（Access Server）是广域网中拨入和拨出连接的会聚点。如图 5-84 所示，说明了接入服务器如何将多条拨出连接集合在一起接入广域网。

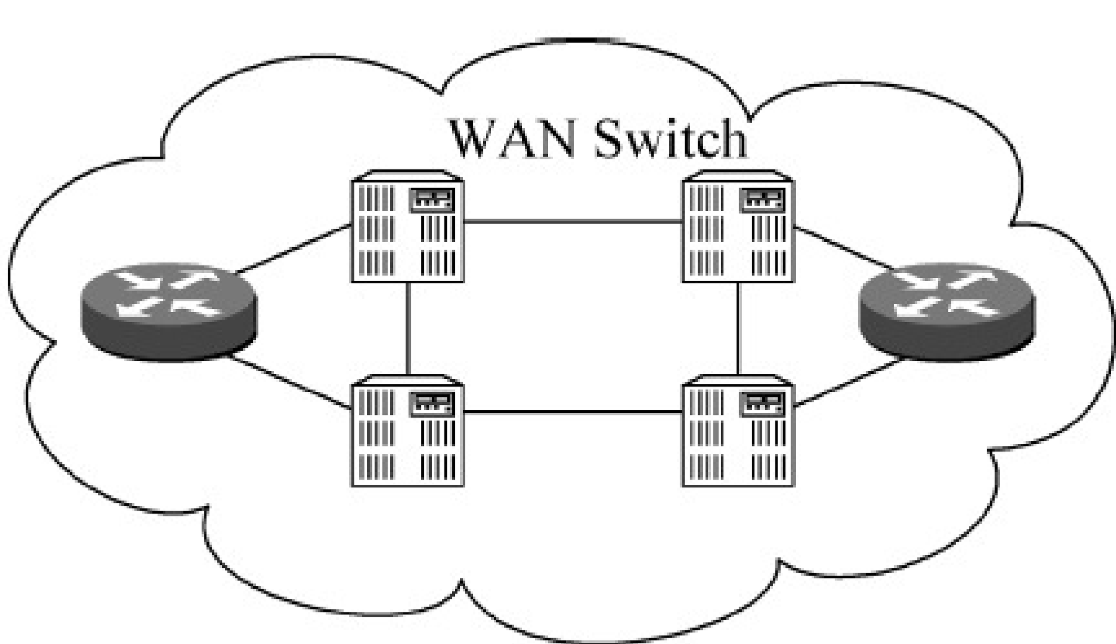


图 5-83　广域网交换机

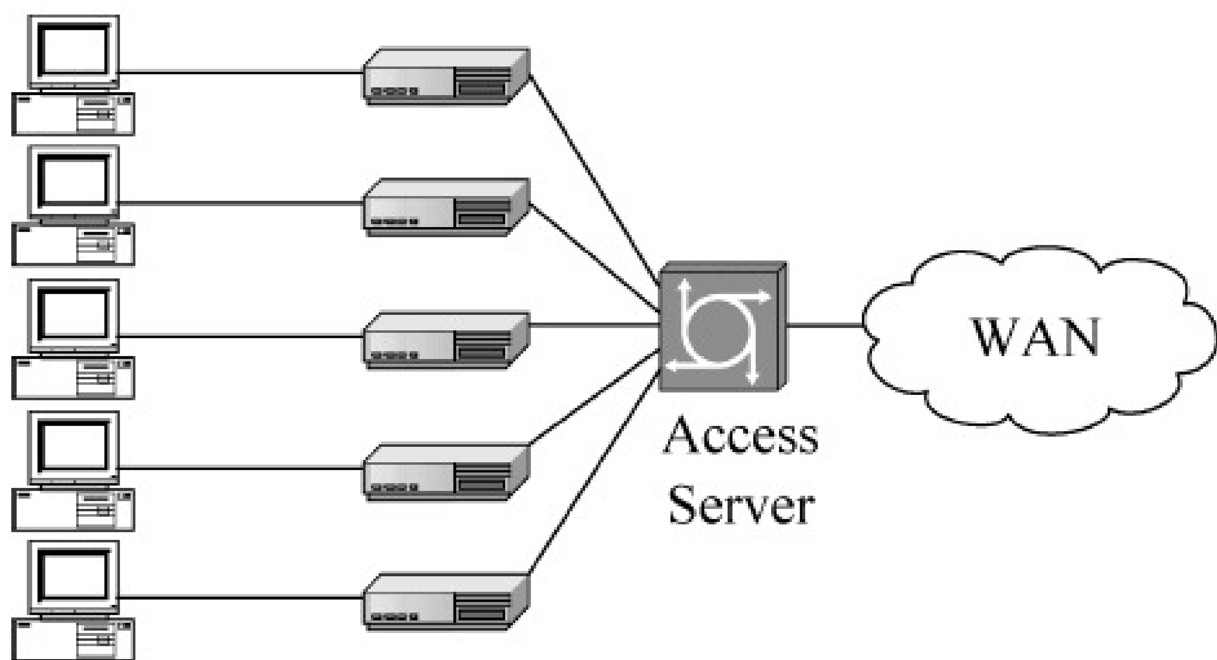


图 5-84　接入服务器

③ 调制解调器

调制解调器(Modem)主要用于计算机与通信介质,数字信号和模拟信号之间的转换,从而能够通过电话线路传送和接收数据信息。在数据发送方,计算机数字信号被转换成适合通过模拟通信设备传送的形式;而在目标接收方,模式信号被还原为数字形式,如图 5-85 所示。



图 5-85　Modem 联网

④ CSU/DSU

信道服务单元(CSU)/数据服务单元(DSU)是类似于数据终端设备到数据通信设备的复用器,可以提供以下几方面的功能:信号再生、线路调节、误码纠正、信号管理、同步和电路测试等,如图 5-86 所示。

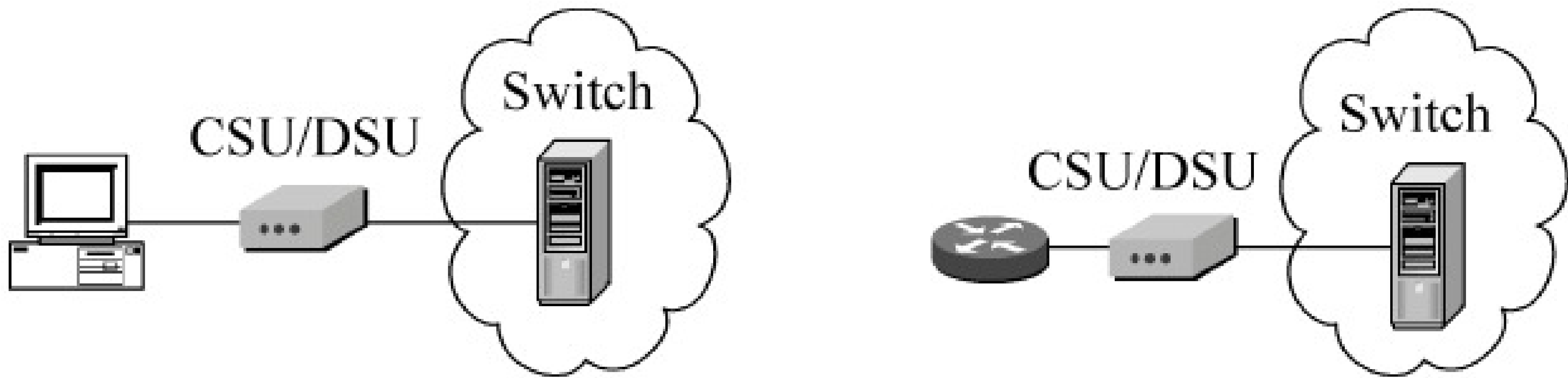


图 5-86　CSU/DSU

⑤ ISDN 终端适配器

ISDN 终端适配器(TA)是用来连接 ISDN 基本速率接口(BRI)到其他接口(如 EIA/TIA-232)的设备(如图 5-87 所示)。从本质上说,ISDN 终端适配器就相当于一台 ISDN 调制解调器。

2. 广域网协议

广域网协议在地域分布很远、很分散,以至于无法用直接连接来接入局域网的场合,广域网(WAN)通过专用的或交换式的连接把计算机连接起来。这种广域连接可以是通过公众网建立的,也可以是通过服务于某个专门部门的专用网建立起来的。相对来说,广域网显得比较错综复杂,主要是用于广域传

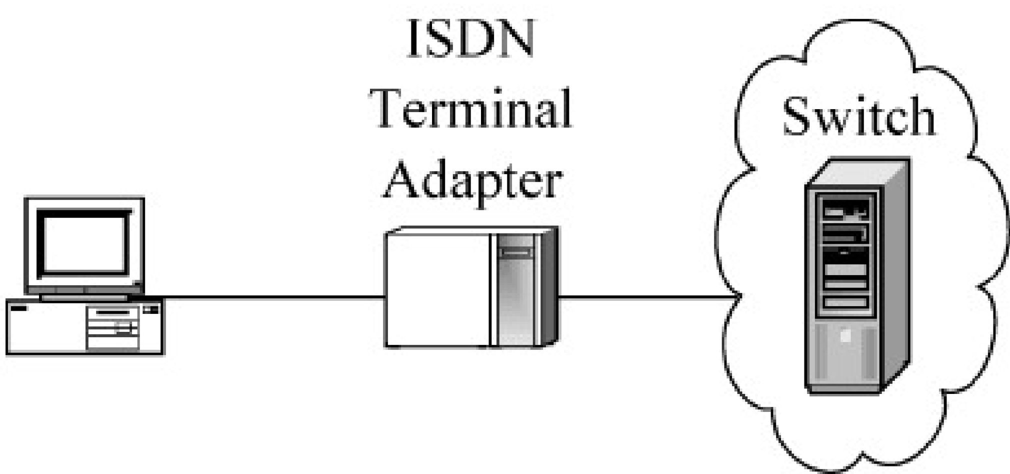


图 5-87　ISDN 联网

输的协议比较多：PPP(点对点协议)、DDN,ISDN(综合业务数字网)、X.25、FR(帧中继)、ATM(异步传输模式)等。

(1) PPP 点对点协议

PPP 点对点协议主要用于“拨号上网”这种广域连接模式。一般来说，一些无法使用专门的网络线连接的双方(比如说家庭用户、移动用户)需要广域相连接的时候，就可以借助分布最广的公用交换电话网来实现。当要浏览互联网上的网页的时候，首先通过调制解调器连接到电话线上，然后将在远方服务器的内容通过电话线传送到自己的计算机中。或者当大家要发送电子邮件的时候，就可以将写好的电子邮件从电话线中传送出去。另外，两个不同城市的两台计算机要互相传送数据，也可以通过装在两台计算机上的调制解调器，让其中一台呼叫另一台(拨打它的电话号码)，通过建立点对点的连接来实现的。迄今为止，拨号上网还是绝大多数的家庭用户和小型办公室用户广域连接的一种最常用的手段。但是因为传输线路是模拟线路，所以传输速度较慢。

用户接入 Internet，在传送数据时都需要有数据链路层协议，其中最为广泛的是串行线路接口协议(SLIP)和点对点协议(PPP)。SLIP 协议仅是一个包协议，提供在串行通信线路上封装 IP 数据包的一种方法，即将 IP 数据包在串行线路上转换成帧格式，以便远程用户通过电话线和 Modem 能方便地接入 TCP/IP 网络。因为它不提供寻址、包类型标识、差错控制或压缩机制，因此，协议简单，非常容易实现。由于 SLIP 连接的双方都需要知道对方的 IP 地址，通信时，需要将各自的当前 IP 地址通知对方，主要用于低速(不超过 19.2kbps)的交互性业务，它并未成为 Internet 的标准协议。为了改进 SLIP，人们制定了点对点 PPP 协议。

① PPP 三大成就

a) 明确地划分出一帧的尾部和下一帧的头部的成帧方式。这种帧格式也处理错误检测工作。

b) 当线路不再需要时，挑出这些线路，测试它们，商议选择，并仔细地再次释放链路控制协议。这个协议被称为链路控制协议 LCP(Link Control Protocol)。

c) 用独立于所使用的网络层协议的方法来商议使用网络层的哪些选项。对于每个所支持的网络层来说，所选择的方法有不同的网络控制协议 NCP(Network Control Protocol)。PPP 帧不仅能通过拨号电话线发送出去，而且还能通过 SONET 或真正面向位的 HDLC 线路(即路由器与路由器相连)发送出去。

② PPP 协议组成

PPP 协议有三个组成部分。

a) 一个将 IP 数据报封到串行链路的方法。PPP 既支持异步链路(无奇偶校验的 8 比特数据)，也支持面向比特的同步链路。

b) 一个用来建立、配置和测试数据链路的链路控制协议 LCP(Link Control Protocol)。通信的双方可协商一些选项。在“RFC 1661”中定义了 11 种类型的 LCP 分组。

c) 一套网络控制协议 NCP(Network Control Protocol)，支持不同的网络层协议，如

IP、OSI 的网络层、DECnet、AppleTalk 等。

③ PPP 链路工作过程

a）LCP 协商。进行 LCP 协商的内容包括工作方式是 SP 还是 MP、验证方式和最大传输单元等。

b）建立阶段。LCP 协商过后就进入建立阶段，此时 LCP 状态为“打开”，表示链路已经建立。

c）验证阶段。如果配置了验证（远端验证本地或者本地验证远端）就开始 CHAP 或 PAP 验证。如果验证失败进入终止阶段，拆除链路，LCP 状态转为“断开”；如果验证成功，就进入网络协商阶段 NCP，此时 LCP 状态仍为“打开”，而 IPCP 和 IPXCP 状态从“初始”转到“请求”。

d）网络协商阶段。NCP 协商后将选择和配置一个或多个网络层协议。每个选中的网络层协议配置成功后，该网络层协议就可通过这条链路发送报文了。NCP 协商支持 IPCP 和 IPXCP 协商。IPCP 协商包括协商双方的 IP 地址；IPXCP 协商包括双方的网络号和节点号。

e）链路保持阶段。经建立的链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件中断链路，此链路不被拆除。

f）拆除链路阶段。当用户通信完毕时，NCP 释放网络层连接，收回原来分配出去的 IP 地址。接着 LCP 释放数据链路层连接，最后释放的是物理层的连接。

（2）ISDN 综合业务数字网

ISDN 经历了一个极为漫长的“进化”过程。如果常看一些网络界的时报，一定不会在 10 年之前就对它有所耳闻。在它出现的时候，远程通信界的专家们都声称它是未来的公共电话、电信接口。但是它的不够经济却严重地阻碍了它的广泛应用。中国电信用了一个形象的名字“一线通”描述出它的特点：ISDN 将数据、声音、视频信号集成进一根数字电话线路，提供有效、经济的途径，将用户与高带宽数字服务相连。

① ISDN 的通信技术

在 ISDN 中，用户设备与 ISDN 局之间通过一个数字管道连接。数字管道用位流的时分复用支持多个独立的通道。

a）信道

ISDN 定义了三种信道：B 信道、D 信道和 H 信道。

B 信道，也称载体信道，其速率为 64kbps，是基本的用户信道。B 信道用于承载数据、数字语音或其他低速率的信息。它用全双工的方式运载数字信息，并在一个 B 信道中以端对端的方式进行传输。

D 信道，也称数据信道，其速率为 16kbps 或 64kbps，视用户的需要而定。用于传输呼叫用户的数字信令或某些低速率的数据。

H 信道，也称混合信道或数字信道，其速率为 384kbps、1536kbps 或 1920kbps，适合于视频或远程会议等高速率的应用业务。

b）用户接口

ISDN 有两种标准接口：基本速率接口 BRI 和基群速率接口 PRI。

基本速率接口。基本速率接口 BRI 包括两个速率为 64kbps 的 B 信道和一个速率为 16kbps 的 D 信道。允许用户在传输模拟电话的数字管道中进行纯数字通信，通常用于小容量系统。

基群速率接口。基群速率接口 PRI 包括 23(或 30)个速率为 64kbps 的 B 信道和一个速率为 16kbps 的 D 信道。一个 PRI 可以支持多达 23 个或 30 个源与目标进行全双工通信。通常用于大容量系统。PRI 的终端用户通常是一个有 ISDN 功能的数字专用分支交换机或一个主计算机。

② ISDN 分类说明

ISDN 可分为 N-ISDN(窄带 ISDN)和 B-ISDN(宽带 ISDN)两种。

常用于家庭及小型办公室的是 N-ISDN，它提供的基本速率接口(BRI)服务由两个 B 信道和一个 D 信道组成(2B+D)，其中 B 信道为 64kbps，D 信道为 16kbps。

B-ISDN 即 ATM 网，是电路技术与分组技术的组合，它采用同步数字体系 SDH/同步光纤网 SONET 为传输媒介，以异步传输方式为通信标准。B-ISDN 提供的主要速率接口(PRI)则根据不同的国家而不尽相同。在北美、日本为 23 个速率 64kbps 的 B 信道和 1 个速率也为 64kbps 的 D 信道，总速率为 1.544Mbps，即 23B+D。在欧洲、澳洲及其他国家，一般则是由 30 个速率 64kbps 的 B 信道和 1 个速率也为 64kbps 的 D 信道构成，总的接口速率可达到 2.048Mbps，也就是 30B+D。

(3) xDSL

xDSL 是 DSL (Digital Subscriber Line)的统称，即数字用户线路，是以铜电话线为传输介质的传输技术组合。DSL 技术主要分为对称和非对称两大类。

① HDSL(高速对称 DSL)：是 xDSL 技术中最成熟的，它利用两对双绞线传输，支持 $N\times64$kbps 和多种速率，最高可达 1544kbps(E1)速率。

② SDSL(对称 DSL)：利用单对双绞线传输，支持多种速率，最高到 2048kbps/1544kbps(T1/El)。

③ MVL：Paradyne 公司开发的低成本对称 DSL 传输技术，可以提供上下行 768kbps，传输距离可达 6km。

④ ADSL(非对称 DSL)：利用现有铜双绞线(即普通电话线)，提高到 8Mbps 下行速度，1Mbps 上行速度，传输距离达 3km 到 5km。

(4) DDN 数字专线

数字数据网 DDN 是利用数字信道传输数据信号的数据传输网，其传输媒介有光缆、数字微波、卫星信道以及用户端可用的普通电缆和双绞线。DDN 主要向用户提供端到端的数字型数据传输信道，既可以用于计算机远程通信，也可传送数字化传真、数字语音、图像等各种数字化业务。由数字通道、DDN 节点、网管控制和用户环路 4 个部分组成。

① DDN 的特性

a) DDN 为同步数据传输网，不具备交换功能。但具有半永久性连接，可根据与用户所订协议，定时接通所需路由。

b）传输速率高，网络时延小。DDN采用同步转移模式的数字时分复用技术，用户数据信息依据已约定的协议，在固定的时隙以预先设定的通道带宽和速率，顺序传输到目的终端，在目的终端无须重组信息。目前传输速率可高达155Mbps，平均延时小于450μs。

c）DDN为全透明网。DDN支持所有的规程，可支持网络层以及其上的任何协议，从而可满足数据、图像、声音等多种业务的需要。

② PCM设备

PCM设备是DDN网络的大容量设备。目前有两种制式，一是T1制式，美、日等国使用，PCM24路一次群设备；另一种是E1制式，西欧等使用，PCM30/32路一次群设备。我国采用E1制式。

③ 网络结构

DDN网络按网络的组建、运营、管理、维护的责任和地理区域，分为一级主干网、二级主干网和三级本地网。各级网络再细分，组建多功能层次的网络。

我国邮电部于1994年10月完成了全国数字数据骨干网的一期建设。这个网络是利用光纤、数字微波或卫星数字交驻连接设备组成的数字数据业务网。这些数字线路用于出租给最终用户。我国的DDN网络结构如下。

a）一级主干网。设置在省会城市。根据电路组织、网络规模、安全和业务等因素，选择适当位置的节点作为枢纽节点，枢纽节点具有E1数字通道的汇接功能和E1公共备用数字通道功能。

b）二级主干网。一般建立在省内，提供省内长途和出入省的DDN业务。

c）三级本地网。指一个城市或某个区域范围内的网络。本地网直接为其用户提供本地和长途DDN业务。可以根据网内的网络规模和业务量划分多个层次的网络。它的小容量节点直接设在用户处。

对于某些需要更高的传输速度和质量的用户，可以租用DDN线路来实现。租用了DDN线路，就等于在用户与电信局端直接用一条定制带宽的专用电话线路相连，显然这能大大提高整个数据传输的稳定性和速度。在DDN的客户端需要一个称为DDN Modem的CSU/DSU设备，以及一个路由器，它的价格与DDN线路的带宽相关，一般来说，开通一个DDN客户端的费用在1.5万元左右。

（5）X.25

X.25是历史最悠久的广域数据传输协议。X.25协议工作在公用数据网上，是公用数据网络上终端以分组方式进行操作的数据终端设备（DTE）和数据电路终端设备（DCE）之间的接口，在网络中，DTE通常是计算机；DCE通常是调制解调器、网关和网桥等网络互联设备。

尽管X.25协议是所有广域数据传输协议的鼻祖，而且也曾经为广域传输做出了很大的贡献，然而现在它似乎已经走到了尽头，X.25的应用越来越少了。

（6）FR帧中继（Frame Relay）

作为X.25网络协议的发展，帧中继是一种高性能的广域网协议。它是X.25的一个简化版本，省去了X.25的一些强制功能，如提供窗口技术和数据重发功能，这是因为帧

中继的设计是以网络的传输环境已经有了很大的提高为前提的。

1990 年，Cisco、Digital Equipment、Northern TeleCom 和 StartaCom 等公司组成一个联合体，共同开发了帧中继技术。此后，帧中继技术有了迅猛发展。从整个连接上，帧中继与 X. 25 相当类似。但它在数据分组确认和差错校验方法上有了很大的简化，而且分组的转发也有了改变。帧中继只要接到分组头，就开始转发，这样进一步提高了速度。但是，需要强调的是，帧中继在网络环境不好的情况下，将无法像 X. 25 那样提供较好的传输质量，而且可能会使传输质量急剧下降。

① 帧中继技术是一种快速分组交换技术，归纳为以下几点：

- 帧中继技术主要用于传递数据业务，它将数据信息封装为帧形式进行传送。
- 帧中继采用虚电路技术，在一个物理连接上可复用多个逻辑连接，能充分利用网络资源。
- 帧中继网的通信处理简化，得到了低延迟和高吞吐量的性能。
- 帧中继的帧信息长度比 X. 25 分组长度要长，最大可达 1600B/帧，且长度是可变的，适合于传送突发业务。
- 帧中继可用作低成本、高速度的主干广域网，连接那些不承担实时通信任务，但会发送突发性数据的局域网。

② 帧中继配置

企业网申请帧中继时，局端提供 DLCI 号和接入的 LMI 类型，局端是 DCE，客户端是 DTE。设局端提供的虚电路号 DLCI 是 16 和 17，本地管理类型接口 LMI 是 Cisco。设置内容：连接端口的 IP 地址，指定 lmi 类型，设置虚电路号。

例如：

```
Router(config)#int s0/0
Router(config-if)#ip address 172.16.20.1 255.255.255.0
Router(config-if)#encap frame-relay
Router(config-if)#frame-relay lmi-type cisco
Router(config-if)#frame-relay dlci 16
```

如果在实验室条件下配置帧中继，要求用一个路由器做继交换机 switching。

```
Router(config)#frame-relay switching
```

当要求一点对多点时，可以使用子接口的帧中继设置。

（7）ATM 网

异步传输模式 ATM 是一种重要的广域网技术，它吸取了分组交换高效率和电路交换高速率的优点，是一种快速分组交换，也称为信元交换。

ATM 采用类似于分组交换中的信息封装方式，将需要传输的信息切割并封装在一个统一格式的信元的信息分组中，然后在网络上传递，到达接收端后还原为本来的格式。

每个信元的长度为 53 个字节，由 5 字节的信头和 48 字节的信息段组成。信头为寻址等信息，信息段装入被分解成数据块的各种不同业务的用户信息和其他管理信息。

① ATM 协议参考模型

用户面：提供用户信息的传输。控制面：负责呼叫控制和连接控制功能。管理面：负责网络维护和完成运行功能。面管理：执行与整个系统有关的管理功能。层管理：处理运行和维护功能。

物理层：主要是传输信息；ATM 层：主要完成交换、路由及多路复用；ATM 适配层 AAL：主要负责与较高层信息的匹配。

a）物理层：由两个子层组成，物理介质子层和传输汇聚子层。

物理介质子层支持纯粹与介质有关的位功能。传输汇聚子层把 ATM 信元流转换成在物理介质上传输的位，如把帧匹配成在传输系统中所用的格式（SDH、PDH、基于信元的格式）、信元定界等功能。

b）ATM 层：基本功能是负责生成信元，它不管载体的内容，且与服务无关。主要功能有多路复用、多路复用分解、信元 VPI、VCI 的转换，信元头的产生和去除，流控。

c）ATM 适配层 AAL：由两个子层组成，分段和重组子层（SAR），把高一层的信息单位分段成 ATM 信元，或者把 ATM 信元重组成高一层的信息单位；汇聚子层（CS）与服务有关，可以完成的功能有信报标识和时钟恢复等。

② 信元类型

a）空信元（物理层）：为了使信元流的速率与传输系统可用的有效负载容量相匹配而在物理层插入或除去的信元。

b）有效信元：没有头差错的信元或已经由头差错控制进程修正过的信元。

c）无效信元（物理层）：有头差错且尚未由头差错控制进程修正的信元。

d）指定的信元（ATM 层）：使用 ATM 层服务为应用提供服务的信元。

e）非指定的信元（ATM 层）：尚未指定的信元。

知识拓展——C/S 结构与 B/S 结构

1. 什么是 C/S 结构

C/S（Client/Server）结构，即大家熟知的客户机和服务器结构。它是软件系统体系结构，通过它可以充分利用两端硬件环境的优势，将任务合理分配到 Client 端和 Server 端来实现，降低了系统的通信开销。目前大多数应用软件系统都是 Client/Server 形式的两层结构，由于现在的软件应用系统正在向分布式的 Web 应用发展，Web 和 Client/Server 应用都可以进行同样的业务处理，应用不同的模块共享逻辑组件；因此，内部的和外部的用户都可以访问新的和现有的应用系统，通过现有应用系统中的逻辑可以扩展出新的应用系统。这也就是目前应用系统的发展方向。

传统的 C/S 体系结构虽然采用的是开放模式，但这只是系统开发一级的开放性，在特定的应用中无论是 Client 端还是 Server 端都还需要特定的软件支持。由于没能提供用户真正期望的开放环境，C/S 结构的软件需要针对不同的操作系统开发不同版本的软件，加之产品的更新换代十分快，已经很难适应百台计算机以上局域网用户同时使用。而且代价高，效率低。

2. 什么是B/S结构

B/S(Browser/Server)结构即浏览器和服务器结构。它是随着Internet技术的兴起，对C/S结构的一种变化或者改进的结构。在这种结构下，用户工作界面是通过WWW浏览器来实现的，极少部分事务逻辑在前端(Browser)实现，但是主要事务逻辑在服务器端(Server)实现，形成所谓三层3-tier结构。这样就大大简化了客户端计算机载荷，减轻了系统维护与升级的成本和工作量，降低了用户的总体成本(TCO)。以目前的技术看，局域网建立B/S结构的网络应用，并通过Internet/Intranet模式下数据库应用，相对易于把握、成本也是较低的。它是一次性到位的开发，能实现不同的人员，从不同的地点，以不同的接入方式(比如LAN，WAN，Internet/Intranet等)访问和操作共同的数据库；它能有效地保护数据平台和管理访问权限，服务器数据库也很安全。特别是在Java这样的跨平台语言出现之后，B/S结构管理软件更是方便、快捷、高效。

3. C/S与B/S的区别

(1) 硬件环境不同

C/S一般建立在专用的网络上，小范围里的网络环境，局域网之间再通过专门服务器提供连接和数据交换服务。B/S建立在广域网之上 的，不必是专门的网络硬件环境，例如电话上网，租用设备，信息自己管理，有比C/S更强的适应范围，一般只要有操作系统和浏览器就行。

(2) 对安全要求不同

C/S一般面向相对固定的用户群，对信息安全的控制能力很强。一般高度机密的信息系统采用C/S结构适宜，可以通过B/S发布部分可公开信息。

B/S建立在广域网之上，对安全的控制能力相对弱，面向是不可知的用户群。

(3) 处理问题不同

C/S程序可以处理用户面固定，并且在相同区域，安全要求高的需求，与操作系统相关，应该都是相同的系统。

B/S建立在广域网上，面向不同的用户群，分散地域，这是C/S无法做到的，与操作系统平台关系最小。

(4) 用户接口不同

C/S多是建立在Windows平台上，表现方法有限，对程序员普遍要求较高。

B/S建立在浏览器上，有更加丰富和生动的表现方式与用户交流，并且大部分难度减低，降低开发成本。

(5) 信息流不同

C/S程序一般是典型的中央集权的机械式处理，交互性相对低。

B/S信息流向可变化，B—B、B—C、B—G等信息流向的变化，更像交易中心。

实训5 共享上网

1. 实训目的

使用宽带路由器实现多用户共享上网。

2. 实训内容

现在很多地方都开通了宽带网络，对于拥有多台计算机的家庭或者小型办公室来说，如果能让多台计算机共享一个账号同时上网，可以充分利用网络带宽。

3. 实训步骤

(1) 设备连接。把宽带接入网线连接到路由器的WAN(广域网)口，然后将计算机连接到路由器的LAN(局域网)口。一般家用路由器的LAN口有4个，如果不够用可接入交换机或路由器等设备。

(2) 登录路由器。一般路由器管理界面的连接IP为“192.168.1.1”，首先配置计算机的IP地址与路由器在同一网段，如“192.168.1.10”。在浏览器中输入路由器管理界面地址“192.168.1.1”进行连接。用户名和密码默认为“Admin”。如需修改密码，修改后重启有效。

(3) 路由器配置。登录路由器后，进入WAN口配置界面，根据实际情况选择连接类型，设置“上网账号”、“上网口令”等信息。重启路由器即可生效。这样所有连接到该路由器LAN口的计算机都可以共享一个宽带账号上网了。

4. 实训要求

(1) 理解共享上网的含义。

(2) 分析路由器的作用。

习　题　5

1. 选择题

(1) 正确的Internet地址是(　　)。

A. 32.230.100.6.15　　B. 10.89.20.5

C. 192.112.36.256　　D. 128.174.5

(2) 目前全球最大的中文搜索引擎是(　　)。

A. Google　　B. 百度　　C. 雅虎　　D. 新浪

(3) 当与匿名FTP服务器建立连接时，一般输入的用户名是(　　)。

A. Internet　　B. Anonymous　　C. Netscape　　D. Password

(4) 电子邮件应用程序实现POP3的主要目的是(　　)。

A. 创建邮件　　B. 发送邮件　　C. 管理邮件　　D. 接收邮件

(5) 下列软件中不能下载文件的是(　　)。

A. IE6.0　　B. Flashget　　C. eMULE　　D. WinRar

(6) 以下说法正确的是(　　)。

A. 发件箱：暂存准备发出的邮件；已删除邮件箱：存放已经发出的邮件

B. 发件箱：暂存准备发出的邮件；已删除邮件箱：存放准备删除的邮件

C. 发件箱：存放已发出的邮件；已删除邮件箱：存放准备删除的邮件

D. 以上都不正确

(7) 通常所说的拨号上网，是指通过(　　)与因特网服务器连接。

A. 微波　　B. 公用电话系统　　C. 专用电缆　　D. 电视线路

(8) 下列 4 项中表示电子邮件地址的是(　　)。

A. ks@183.net　　B. 192.168.0.1

C. www.gov.cn　　D. www.cctv.com

(9) 下列 4 项中主要用于在 Internet 上交流信息的是(　　)。

A. DOS　　B. Word　　C. Excel　　D. E-mail

(10) 发送电子邮件时,如果接收方没有开机,那么邮件将(　　)。

A. 丢失　　B. 退回给发件人

C. 开机时重新发送　　D. 保存在邮件服务器上

2. 填空题

(1) 调制解调器主要有三种________、________和________。

(2) Internet 最早起源于美国国防部的________网络。

(3) 对 Internet 来说,最重要的两个协议被称做________和________,它们把局域网紧密地连接在一起。普通用户经常使用的另一种协议则称为________,它是让个人计算机用户进入 Internet 的技术标准。

(4) WWW 系统是由________、________和________三部分构成的。

(5) ________是一个索引查询系统,它可以帮助查找公共 FTP 服务器上提供的文件。

(6) 要在收藏夹中保存网页,可以通过“收藏”菜单中的________命令来实现。

(7) 在高级搜索中符号“-”的作用是________。

(8) 邮件注册成功后,________不可以更改。

(9) Outlook Express 是一个功能强大的________,它集成在________中。

(10) 可以输入________作为用户名,________作为密码来登录允许匿名登录的 FTP 站点。

(11) 在 Internet 中,允许一台主机拥有________个 IP 地址。

(12) ________是 WWW 中最基本的网页构建语言,它用于标注文档,使得该文档可以在________中显示。

(13) IP 地址是由________和________两部分组成的,IP 地址 127.0.0.1 称为________地址,1.1.1.1 称为________地址。

(14) 有了 DNS,凡域名空间中有定义的域名都可以有效地转换为对应的________地址。

(15) Internet 提供的三大基本服务是________、________和________。

(16) 用户从邮件服务器接收邮件有________和________两种方式。

(17) 为了防止腾讯 QQ 密码被盗用户可以在腾讯网站上申请________服务。

3. 简答题

(1) 对给出的 IP 地址进行判断。

IP 地址为:194.47.21.136,请说明该地址属于哪类地址。该类地址的最大网络的接入数是多少?每个子网最大主机数是多少?如果使用默认的网络掩码,该 IP 地址的网络地址是什么?

(2) 简述当 WWW 用户查询信息时客户浏览器与 Web 服务器的交互过程。

(3) 列出至少两种进入 Internet 的形式。

(4) 电子邮件有哪些使用方式?各方式的优点和缺点是什么?

模块 6　网络的管理

任务 6.1　为小型局域网进行服务器的安装与配置

任务描述：由 1 台服务器和 20 台个人计算机组成客户机/服务器网络。要使网络正常运行，需要对客户端个人计算机和服务器进行相应软件的安装与配置。读者在本书前面部分已经了解了个人计算机的配置，本章将对服务器上软件的安装与配置进行详细介绍。下面将本任务分解为 5 个子任务进行叙述。

6.1.1　了解网络操作系统

在完成了网络的物理搭建之后，需要对网络设备进行软件的安装与配置。首要的就是为服务器安装网络操作系统。根据要组建的网络用途及网络的类型，选择相应的网络操作系统。

网络操作系统(Network Operation System)负责整个网络系统的软硬件资源的管理和控制。通过网络操作系统实现对网络通信和任务的调度，维护网络系统的安全性。由于网络操作系统主要运行于服务器上，所以有时候把它称之为服务器操作系统。

网络操作系统的特征如下：

(1) 提供支持协议、硬件监测、处理器、应用程序等基本操作系统的服务。

(2) 提供文件、打印、Web 服务、支持和复制服务。

(3) 支持 Internet 网络。

(4) 提供服务名称和目录。

(5) 提供安全特征服务，如授权、认证、登录限制和访问控制。

(6) 提供用户管理支持远程访问、系统管理、图形接口管理、登录、下载。

(7) 容错及高效性系统。

经过近几十年的发展，网络操作系统经历了从对等结构到非对等结构的发展过程。

1. 对等结构的网络操作系统

在对等结构的网络中(如图 6-1 所示)，所有的网络节点地位都是平等的，任意两个节点都可以直接进行通信，每个节点中的资源都可以共享。在对等网中使用对等结构的操作系统，由于对等网中不需要专门的服务器，所以对等结构的网络操作系统功能相对简单，使用比较方便而且组建网络的成本比较低。其不足之处是，由于网络中的每个节点既要完成一些工作站的任务如事务处理，又要向其他节点提供网络资源，承担较重的网络通信管理和共享资源管理任务，加重了节点的负担，造成了信息处理能力的下降。另外在网络中的资源文件等存放的位置分散，不易管理且保密性不高。因此对等结构的网络操作

系统适合于一些网络规模较小、信息交换量不大、安全性要求不高的网络。

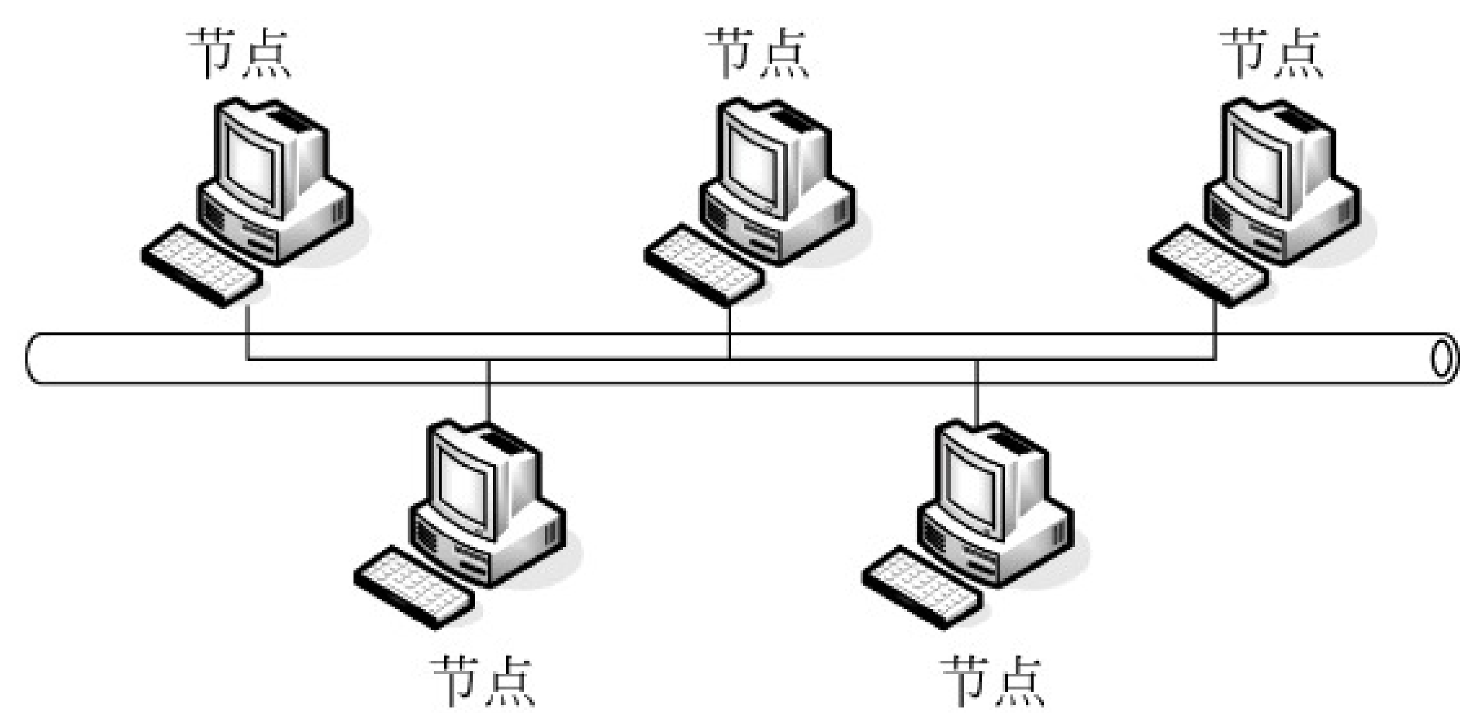


图 6-1 对等结构网络

2. 非对等结构的网络操作系统

非对等结构的网络在工作时，服务器运行的网络操作系统的功能与性能，直接决定着该网络服务的功能强弱以及系统的安全性，因此它是系统的核心。客户机只是运行一些作为工作站服务的功能。

客户端程序向服务器提出某种服务申请，服务器程序运行在服务器上，当接到客户端的请求之后，根据系统的功能，运行该服务操作，完成后将结果返回给客户端程序，而客户端通过输出设备显示给用户。例如，在网络中，用户通过客户端计算机运行浏览器服务，想要浏览某网站主页，向网络中的服务器发出请求，服务器在接收到该客户程序的请求之后，执行相关操作，将请求的页面返回到客户端，这时候用户通过客户端计算机就能看到请求的主页了。

采用非对等结构的网络模式有以下优点：由于服务器程序和客户程序运行在不同的主机上，从而简化了程序的运行过程，降低了硬件的要求，使计算机的性能得到充分的发挥，提供良好的网络服务；客户程序也可以与多个服务器相连接，使用户根据需要灵活地访问多台服务器。

目前应用较多的网络操作系统有 Windows 系列、UNIX 系统、Linux 系统和 NetWare 系统等。

（1）Windows 系列

Windows 系列操作系统是全球最大的软件开发商——Microsoft（微软）公司开发的。由于其良好的人机图形用户界面，使得用户很容易掌握，它不仅仅在个人版的操作系统中占有绝对的优势，在网络操作系统中也具有非常强的实力。但是由于 Windows 系列对服务器的硬件要求较高，且稳定性、安全性相对较弱，所以一般用在中低档的服务器中。

Windows 系列网络操作系统的产品主要有：Windows NT、Windows 2000 Server、Windows Server 2003 等。

Windows Server 2003 系列继续沿用了 Windows 2000 Server 的优良特性，不仅在可靠性和可用性上有了长足的进步，同时还在可扩展性、可操作性、安全性、可管理性等诸多方面显现出了优异的性能。另外，Windows Server 2003 借鉴了 Windows XP 的易用性、人性化、智能化的特点，并且提供更加稳定的内核，更加丰富的网络服务功能。同时 Windows Server 2003 对.NET Framework 1.1 的完美支持点，提供了开发、部署到管理的最佳解决方案，适用于中小型网络。

Windows Server 2003 的新功能包括：活动目录（Active Directory）、Web 与应用程序服务、Windows 媒体服务、存储管理、安全服务、打印服务、文件服务、管理技术、终端服务、网络与应用程序服务、网络与通信、群集等。Windows Server 2003 有 4 个版本。

① Windows Server 2003 标准版（Standard Edition）。

Windows Server 2003 标准版是一个可靠的网络操作系统，可以迅速方便地提供企业解决方案。它是为小型企业和部门服务器设计的，其可靠性、可伸缩性和安全性，能满足小型局域网构建的要求。其特点如下：

- 支持 4 路对称多处理器系统，4GB 内存，支持超线程。
- 支持文件和打印机共享。
- 提供安全的 Internet 连接。
- 允许集中化的桌面应用程序部署。

② Windows Server 2003 企业版（Enterprise Edition）。

Windows Server 2003 企业版是为中型与大型企业服务器设计的，有 32 位和 64 位两个版本。与 Windows Server 2003 标准版不同，Windows Server 2003 企业版能支持更高性能的服务器，功能更强大，并且可以集群服务器，以便处理更大的任务。它是各种应用程序、Web 服务和基础结构的平台，提供高度可靠性、高性能和出色的商业价值。其特点如下：

- 32 位版本的支持 8 路对称多处理器系统和 32GB 内存。
- 64 位版本的支持 8 路对称多处理器系统和 64GB 内存。
- 支持 8 节点的服务器群集，支持多线程。

注意：服务器群集：几台服务器共同负责原来一台服务器的工作。可以提供负载均衡的能力，同时还可以防止服务器单点故障的产生，也使网络易于扩展。

对称多处理器（SMP）系统。在一个计算机上汇集一组处理器，各处理器共享内存子系统以及总线结构。系统将任务队列对称地分布于多个处理器上从而提高了整个系统的数据处理能力。所有的处理器可以平等地访问内存、I/O 和外部中断。工作负荷能够均匀地分配到所有可用的处理器之上。

超线程。利用特殊的硬件指令，把两个逻辑内核模拟成两个物理芯片，使得单个处理器能进行线程级并行计算，进而兼容多线程操作系统和软件，减少 CPU 的闲置时间，提高运行效率。

③ Windows Server 2003 数据中心版（Datacenter Edition）。

Windows Server 2003 数据中心版是为面向企业的各种任务所倚重的应用程序而设计的，实现了最高可伸缩性和可靠性的设计，支持数据库的关键业务解决方案、企业资源计划软件、大量实时事务处理和服务器合并，是 Windows 系列中功能最强大的系统，其特点如下：

- 是 Microsoft 迄今为止开发的功能最强大的服务器操作系统。
- 支持高达 32 路的 SMP 和 64GB 的 RAM。
- 标准功能是提供 8 节点群集和负载平衡服务。
- 将可用于能够支持 64 位处理器和 512GB RAM 的 64 位计算平台。

④ Windows Server 2003 Web 版(Web Edition)

Windows Server 2003 Web 版是专门为 Web 服务提供的，其功能全面。作为 Windows 系列中的新产品，其特点如下：

- 用于生成和承载 Web 应用程序、Web 页面以及 XML Web 服务。
- 其主要目的是作为 IIS 6.0 Web 服务器使用。
- 提供一个快速开发和部署 XML Web 服务和应用程序的平台，这些服务和应用程序使用 ASP.NET 技术，该技术是.NET 框架的关键部分。
- 便于部署和管理。

(2) UNIX 系统

UNIX 操作系统是一种多用户多任务的操作系统，出现于 20 世纪六七十年代，最早由美国的贝尔实验室制作，早期的 UNIX 系统使用汇编语言写成，后来随着 C 语言的出现，重新用 C 语言编写了 UNIX 系统。由于 C 语言对计算机硬件的依赖程度小，所以 UNIX 操作系统具有非常好的移植性。

UNIX 操作系统支持网络文件系统服务，提供数据等应用，功能强大。这种网络操作系统的稳定性和安全性能非常好，但由于本身的操作多数以命令的方式进行，不容易掌握。所以，UNIX 操作系统多用于大型的企业公司、网站。而在小型的局域网中基本上不会使用。

目前常见的 UNIX 操作系统版本有：AT&T 和 SCO 公司的 UNIX SVR 3.2/4.0/4.2；SUN 公司的 Solaris；IBM 公司的 AIX；HP 公司的 UX 等。

UNIX 操作系统主要有以下特点：

① 安全性高。使用 DOS 和 Windows 的用户，很少有没被计算机病毒感染过的经历。而 UNIX 操作系统在抵御病毒方面，比其他的操作系统要更有优势。UNIX 操作系统在用户权限、文件和目录权限、内存管理等方面都有非常严格的规定，这样使系统的安全性得到了充分保障。另外 UNIX 操作系统在网络信息的保密性，数据的安全备份方面都提供了良好的保护措施。

② 可靠性高。经过多年的实践认证，UNIX 操作系统是一个成熟且比较稳定可靠的系统。因为安装 UNIX 操作系统的主机和服务器几乎可以每天 24 小时，每年 365 天不间断地运行，而不会出现死机现象，这是其他操作系统所不能比拟的。所以现在多数的大型服务器都使用 UNIX 操作系统。

③ 可移植性强。由于现在的 UNIX 操作系统主要是由 C 语言编写的，对硬件的依赖程度比较小，具有良好的可移植性，所以适用于各种硬件。

④ 多用户多任务。UNIX 操作系统支持不同的用户分别在不同的终端上同时进行交互式操作，就像是每个用户自己单独使用主机一样。

⑤ 提供两种用户界面。一是程序级界面，即系统调用界面，用户和程序员可以直接使用命令调用系统。二是操作级界面，为用户提供交互式功能。

⑥ 强大的网络功能。Internet 的基础是 TCP/IP 协议，而 TCP/IP 协议是随着 UNIX 的发展而不断发展和完善的。几乎所有的 UNIX 操作系统都支持 TCP/IP 协议。所以在 Internet 中的服务器里面，绝大多数使用 UNIX 操作系统。

(3) Linux 系统

Linux 操作系统是一种比较新型的网络操作系统,它与前面介绍的 UNIX 系统有很多相似的地方。而它最大的特点是源代码完全公开,用户可以免费获得。

Linux 操作系统最初由芬兰赫尔辛基大学的大学生 Linus Benedict Torvalds 于 20 世纪 90 年代初编写。该系统遵循 POSIX(Portable Operating System Interface,可移植操作系统接口)标准,提供了 UNIX 的编程界面。但是它与 UNIX 及其他的系统不同的是,内核完全重写,是一个免费的、源代码公开的自由软件。

Linux 系统在安全性和稳定性方面做得非常优秀,现在主要应用于中高档服务器。目前,单机版的 Linux 版本主要包括:RedHat(红帽子)、红旗 Linux 等。

Linux 是目前三大主流操作系统之一。因为 Linux 在成本、性能和可靠性等方面的优势,在市场上很受欢迎。

Linux 操作系统的特征如下。

① 免费、源代码开放。Linux 是免费的,获得 Linux 的渠道很多而且方便,Linux 开放源代码,让使用者能控制源代码,安全并且易扩展。

② 多用户多任务。Linux 系统可以同时被多个用户使用,每个用户对自己的资源有特定的权限,互相不影响。且系统同时能执行多个任务和程序,各个程序独立运行互不影响。

③ 出色的速度性能和稳定性。Linux 系统对硬件的要求不高,可以把处理器的性能发挥到极致。而且系统可以连续运行数年时间不会出现死机现象。

④ 网络功能强大。Linux 系统是在 Internet 基础上产生和发展起来的,在相同的硬件条件下,它通常比 Windows NT、Novell 和大多数 UNIX 系统的性能更加优越。

⑤ 兼容性好。由于 Linux 系统支持 POSIX 标准,所以与 UNIX 在标准上没有多少区别,因此大多数的 UNIX 应用程序也可以在 Linux 系统下运行。

Linux 的发行版本主要有两种,内核版本和发行套件版本。内核版本就是在 Linus 领导下的开发小组研制出的系统内核版本号。一些公司或厂家将 Linux 系统内核与应用软件包装起来发行,即发行套件。发行套件版本因发行者的不同而不同,所以版本很多,目前有 300 多种。

(4) NetWare 系统

NetWare 网络操作系统是由 Novell 公司开发的,它也是一个多用户多任务的网络操作系统。NetWare 是一个开放的网络服务器平台,可以方便对其进行扩充。NetWare 系统具有兼容 DOS 命令,而且它的应用环境与 DOS 相似,对硬件的要求较低。

NetWare 网络操作系统是在局域网的基础上设计的,适用于小型的网络。它不同于一般的网络操作系统需要安装完整的协议和通信传输功能,它具有所有的操作系统的职能,是一个围绕核心调度的多用户共享资源的系统。NetWare 网络操作系统不仅可以支持相同协议的网络接口卡,也可以使用不同协议的网络接口卡,将这些网络接口卡连成一个网络,然后再将这几个网段连接起来形成更大的网络。

NetWare 网络操作系统的主要特点如下。

① NetWare 网络系统为用户提供强大的安全措施。对于网络用户而言,安全性是一

个非常重要的指标。NetWare 网络操作系统支持对用户的口令、密码的管理、文件和目录管理、目录权限以及对用户登录站点和时间的限制等功能。

② 具有系统容错的可靠性措施。局域网的可靠性在很大程度上取决于对服务器硬件故障的检错和纠错能力,能有效地备份数据。NetWare 系统对文件服务器的共享硬盘采取了较多的可靠性措施。

③ 开放的网络软件开发环境。开放数据链路接口是 NetWare 网络系统的一项重要的网络互联技术,以 NetWare 系统为开放式服务器,支持多种通信协议和多种设备驱动程序,一起组成异构的计算机网络。

3. 网络操作系统的选择

组装计算机网络时,应从网络自身的特点出发,权衡各方面的利弊,选择合适的操作系统。

(1) 选择操作系统的依据

① 安全性。选择操作系统时一定要考虑它的安全性。要求网络系统本身具有抵抗病毒的能力,同时所选择的操作系统必须有大量的防杀病毒软件作为保障。

② 可靠性。一个成熟的操作系统必须具有高度可靠性。

③ 易用性。易于使用是对操作系统的最起码要求。安装简单、界面友好、升级容易、对硬件要求不能过高,这些都是选择操作系统时必须考虑的因素。

④ 可维护性。要求用户通过简单的学习和培训就能胜任网络的日常维护工作。同时,网络的维护成本要低。

⑤ 可管理性。可管理性是系统以及第三方软件对管理的支持。

⑥ 可集成性与可扩展性。可集成性是指网络操作系统对硬件及软件的兼容能力。网络操作系统作为不同软硬件资源的管理者,应具有广泛的兼容性,尽可能多地管理各种软件硬件资源。可扩展性就是对现有系统要有足够充分的扩展能力。可扩展性保证今天的投资能适应今后的发展。

(2) 小型局域网操作系统应具备的特点

① 操作系统的安装界面友好,安装过程简单。

② 网络的维护要方便,排除故障的方法和过程也要相对简单。

③ 不同操作系统之间的兼容性要好。

④ 所选操作系统要支持广泛的应用软件,使得主流应用软件都能在该操作系统下良好稳定地运行。

(3) 选择合适的操作系统

组建小型或中型网络,Windows Server 2003 应该是比较好的选择。

组建全新网络,规模又比较大,有远程互联的需要,并对安全性和稳定性有较高的要求,则选择 UNIX。

如果已经具备了 UNIX 的操作经验,且服务器配置不太高,则可以选择 Linux。

如果组建几台计算机的网络时,安全性要求不高,只是在单机基础上加入网络服务功能,使用 Windows XP 是不错的选择。

按照任务要求,我们选择 Windows Server 2003 操作系统作为本网络的操作系统。

6.1.2 Windows Server 2003 的安装

任务分解：服务器操作系统的安装分为升级安装和全新安装两种形式。安装方式也有不同情况，下面分别进行介绍。

1. 光盘引导全新安装

设置为计算机第一引导盘为光盘，插入安装盘；计算机自检后，选择“安装/修复Windows Server 2003”选项；按F8键接受协议；然后按下列步骤执行。

(1) 重新进行分区或者创建新的分区，若要创建新分区，选择“未划分的空间”，按C键。

(2) 选择Windows要安装的分区，按Enter键，选择分区格式“NTFS格式”。系统自动格式化分区并进行安装文件的复制。

(3) 机器重新启动后(将安装光盘暂时取出)，系统自动检测计算机硬件配置，依次完成收集信息、动态更新、准备安装、安装Windows Server 2003等。

(4) 按系统提示依次完成将“区域和语言选项”设置为“中国”；输入单位名称和自己的姓名；输入产品密钥等。

(5) 进行授权模式的选择。

每服务器模式：许可证的数量决定了可以同时连接到服务器的用户数量，该模式适用于用户较多，但同时访问较少的情况。

每设备或每客户：有许可证的用户可以访问任何一台服务器，适用于有多台Windows Server 2003服务器的情况，用户也可以同时访问多个服务器。

这里选择“每服务器模式”，并发用户设置为“20”。

(6) 输入计算机名称，如“XXGC-610”，输入管理员密码(管理员为Administrator)，输入管理员密码时注意安全性。

(7) 进行日期和时间的设置；网络设置(选择典型设置)，安装完成后重新设置。

(8) 选择所在的工作组或计算机域。

由于这里是安装的第一台服务器，还没有设置域，选择服务器是WorkGroup工作组中的成员。最后完成文件复制、开始菜单安装、注册组件等工作。

2. 升级安装

启动原系统后，将安装盘插入，自动运行安装程序，选择安装Windows Server 2003，安装类型选择“升级”即可。

3. 从网络安装

将安装盘下“I386”文件夹下的文件复制到服务器上，设置为共享文件夹，通过“网上邻居”，访问其中的“winnt32.exe”即可。

4. 无人值守安装

要进行无人值守安装需要生成自动应答文件，自动应答文件的生成步骤如下：

(1) 将安装光盘的“\support\tools\deploy.cab”文件解压缩，执行其中的“setupmgr.exe”文件，打开安装管理器。

(2) 选择创建新文件；安装的类型选择“无人参与安装”，选择相应的Windows

Server 2003 版本，用户交互类型选择“全部自动”，选择分布共享方式“从 CD-ROM”或“从网络安装”。

(3) 设置安装时的各种需要输入的参数。

(4) 设置完成后产生两个文件：自动应答文件(从光盘安装时为“winnt. sif”，从网络上安装时为“unattend. txt”)、一个自动批处理文件“unattend. bat”。

(5) 执行创建的批处理文件或者使用命令：

Winnt32/s G:\i386 /unattend: D:\unattend. txt 进行无人值守安装。

5. 优化设置

Windows Server 2003 安装后，可以进行一些设置，提高运行速率等。

(1) 提供系统反应灵敏度

① 在 Windows Server 2003 中运行图像等软件，系统的反应速度变慢。可以用下面的方法提高系统的反应灵敏度。

② 鼠标右击“我的计算机”图标，选择快捷菜单中的“属性”选项。

③ 在“系统属性”对话框中，打开“高级”选项卡，单击“性能”域中的“设置”按钮。

④ 在“性能选项”对话框中，打开“高级”选项卡，在“处理器计划”区域选择“程序”单选按钮。在“内存使用”区域，选择“程序”单选按钮，单击“确定”按钮。

⑤ 在“虚拟内存”区域，单击“更改”按钮。在弹出的“虚拟内存”对话框中，选择系统分区，再选择“无分区文件”单选按钮，单击“设置”按钮，在弹出的对话框中选择“是”按钮。选择一个非系统分区，选择“自定义大小”单选按钮，输入数据，单击“设置”按钮，单击“确定”按钮。重新启动计算机。

(2) 改变系统登录页面

① 登录前不按 Ctrl＋Alt＋Del 组合键

执行菜单命令“开始”→“管理工具”→“本地安全策略”，打开“本地安全策略”对话框。

展开“本地策略”下的“安全选项”，双击右侧的“交互式登录：不需要按 Ctrl＋Alt＋Del”选项，在出现的对话框中，选择“已启用”单选按钮，单击“确定”按钮即可。

② 自动登录系统

通过下列步骤，完成自动登录。

执行菜单命令“开始”→“运行”，输入 regedit，单击“确定”按钮。

展开“HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon”项。

右击窗口右侧空白处，从快捷菜单中选择“新建”→“字符串值”，输入字符串名“AutoAdminlogon”，然后双击它，在弹出的“编辑字符串”对话框中，在“数值数据”输入框中输入“1”。

再建立一个名为 DefaultPassword 的字符串值，将该项的值设为管理员密码。

以后登录系统就会以管理员身份自动登录。如果用其他用户登录按 Shift 键就可以了。

③ 取消关机原因

每次关闭系统时，都需要选择关机原因。取消关机原因的步骤如下：

执行菜单命令"开始"→"运行",输入命令 gpedit. msc,单击"确定"按钮,打开"组策略编辑器"窗口。

在窗口中,依次展开"计算机配置"→"管理模板"→"系统"目录,右击窗口右侧的"关闭事件跟踪程序"选项。

选择"已禁用"单选按钮,然后单击"确定"按钮。

④ 激活常用服务

执行菜单命令"开始"→"管理工具"→"服务",打开"服务"对话框。

如果需要使用摄像头、数码相机、扫描仪等影像设备,在窗口右侧双击"Windows Image Acquisition"选项,在出现的对话框中,设置"启动类型"为"自动",单击"应用"→"启动"按钮。

如果要使用 CD 刻录服务,双击窗口右侧的"IMAPI CD_Buring COM Service"选项,在出现的对话框中,设置"启动类型"为"自动",单击"应用"→"启动"按钮。

⑤ 其他优化设置

移动我的文档的位置。右击"我的文档",选择"属性",在"目标文件夹"选项卡中单击"移动"按钮,选择一个目标盘,单击"确定"按钮。

移动 IE 临时文件位置。在"控制面板"窗口中,单击"Internet 选项",在"常规"选项卡的"Internet 临时文件"区域,单击"设置"按钮,选择"移动文件夹",选择目标文件夹,单击"确定"按钮。在出现的提示框中,单击"是"按钮。

DirectX 加速。执行菜单命令"开始"→"运行",输入 dxdiag,单击"确定"按钮。在"显示"选项卡中单击 DirectDraw、Direct3D 和"AGP 纹理加速"三个按钮。在"声音"选项卡中将"硬件的声音加速级别"滚动条拉到"完全加速"。

6.1.3 在服务器上创建用户账户并分配用户权限

任务分解:在计算机网络中,用户通过账户访问计算机资源。一个用户账户包括账户名、密码、权限等信息,这些信息是存储在计算机中的,是网络上的个人唯一标识;系统通过账户来确定用户的身份,并赋予用户对资源的访问权限。下面介绍在服务器上创建管理员账户、一般账户、设置用户所属用户组、设置用户组权限等操作。

Windows 识别用户是根据账户在创建时建立的安全标识符 SID(Security ID)来完成的。

用户账户的类型:根据 Windows Server 2003 的工作模式,工作组模式和域模式,用户的账户分为本地账户和域账户。

本地账户只能在本地计算机上登录,按权限访问本地计算机的资源。建立在独立服务器、域中的成员服务器以及客户端上。本地用户分为系统内置账户(包括系统管理员 Administrator:具有本地计算机的最高权限,不能删除也不能禁止该账户的登录;来宾 Guest:为临时访问计算机的用户提供的,不能被删除,但可以禁止登录)和用户建立的账户。

1. 创建账户

以管理员身份登录,执行菜单命令"管理工具"→"计算机管理"→"本地用户和组";

右击左侧窗口中的“用户”文件夹，选择“新用户”命令；输入用户名、全名、描述、密码、确认密码；选择用户登录时密码的限制(用户下次登录时须更改密码、用户不能更改密码、密码永不过期、账户已禁用等)，单击“创建”按钮，完成用户创建。

2. 删除账户

在“计算机管理”窗口中，展开左侧窗口中“本地用户和组”选项，单击“用户”，在右侧选择要删除的账户名右击，选择“删除”即可。

3. 更改用户名和密码

在“计算机管理”窗口中，展开左侧窗口中“本地用户和组”项，单击“用户”，在右侧右击要更名的账户名，选择“重命名”项，可以完成用户账户名的修改。

右击账户名，选择“设置密码”，可以更改用户的密码。用户的密码更改，只能由管理员用户或拥有本账户的用户完成。

4. 创建密码重设盘

用户登录后，按 Ctrl＋Alt＋Del 组合键，单击“更改密码”按钮，选择“备份”按钮，输入密码，单击“下一步”按钮，系统创建密码重设盘。

利用密码重设盘修改密码：用户登录不上时，在登录失败对话框中单击“重设”按钮，按屏幕提示，指明重设盘存放位置，单击“下一步”按钮，输入新密码即可。

5. 禁用与激活账户

在“计算机管理”窗口中，右击要修改的账户，选择“属性”，选中或取消“账户已禁用”复选框，完成禁用与激活账户。

6. 用户组的设置

用户组分为系统内置的本地组和用户自己建立的组。

(1) 系统内置的默认本地组

在 Windows Server 2003 中有如下内置组。

- Administrators：该组成员具有最高权限。
- Backup Operators：备份操作员组，主要进行备份和还原工作。
- Users：用户组，该组成员只具有一些基本的权利，可以运行授权的应用程序，使用网络资源，不可以改变系统的配置。
- Guests：来宾用户组，该组中的用户作为临时使用，只能执行被管理员授权的权限和访问的资源。
- Account Operators：账户操作员，具有修改使用者管理员所属的账号和组的权限。但不能修改 Administrators 和任何的 Operators 组。
- Printer Operators：管理域打印机。
- Server Operators：管理与服务器。
- Replicator：负责域中的文件副职，也可进行目录复制程序。

(2) 用户自己建立的组

在“计算机管理”窗口中，展开左侧窗口中“本地用户和组”项，右击“组”，选择“新建组”选项，输入组名、组的描述；单击“添加”按钮，选择分配到该组的成员，单击“创建”按钮完成用户组的创建。

给用户组设置权限。

7. 账户安全管理

合理使用用户数据库：计算机上所有本地账户和组的安全信息都存储在用户数据库SAM(Security Accounts Managers,安全账户管理器)中,该文件的路径是"%windir%\system32\config\sam",删除本文件,则本地计算机所有账户信息都会丢失,Administrator账户的密码将被设置为空。用户用光盘启动系统后,删除该文件,重设用户。

禁用Guests账户。

少用Administrator账户。

为用户或组指定某些权限：在"管理工具"中,打开"本地安全设置"窗口,选择"本地策略"→"用户权限分配"命令。

设置账户安全策略：在"本地安全设置"窗口中,选择"账户策略",设置其中的"账户锁定策略"和"密码策略"。

6.1.4 建立活动目录和域控制器

任务分解：在服务器上建立域控制器,建立多个域账户,将机房内计算机加入域,设置域用户的权限。

活动目录是一种目录服务,它存储有关网络对象的信息(例如,用户、组、计算机账户、打印机等共享资源),使管理员与用户可以方便地查找和使用网络信息。Windows Server 2003将结构化数据存储作为目录信息逻辑和分层组织的基础。

Windows Server 2003系统引入了全新的活动目录服务,使得Windows Server 2003系统与Internet上的各项服务和协议联系更加紧密。因为它的目录命名方式与域名的命名方式采用一致的层次结构,所以通过DNS进行解析,可以取得与在Internet上通过WINS解析一致的效果。通过一个名称就能访问整个域资源。活动目录也说明了Microsoft在网络结构方面的重点策略转移。活动目录存在于整个系统中。

在网络规划和管理中,如何管理用户、计算机、文件、站点、数据库以及其他的管理对象或资源是一个重要的问题。活动目录是一种分布式的目录服务,利用目录管理网络上的各种对象或资源,并且在目录中存储这些信息。

Active Directory可以实现用户和资源的管理、基于目录的网络服务、基于网络的应用管理等。如分布式管理就是利用活动目录的结构化数据存储,作为信息的层次结构。这些信息分布在多台计算机上,可以提高信息的安全性并保证快速访问和容错,并且无论用户从域中哪台计算机访问信息,都能提供统一的视图。

Active Directory中包括了域名服务DNS、消息队列服务MSMQ、事务服务MT、电子邮件等Internet服务和应用。

与Windows 2000 Server不同,在Windows 2000 Server中,域中的所有域控制器之间都是平等关系,不再有主域控制器和备份域控制器。由于Windows Server 2003采取了动态的活动目录服务,在进行目录复制时不再使用主从方式的复制,而是采取多主复制方式。即在进行复制目录时,对各个对象当中的修改时间进行比较,从而判断出先后顺序,

这样用最新修改的对象属性代替旧的属性，保证每个域控制器上的目录数据库都是最新的。

所以说，Active Directory 在整个 Windows Server 2003 体系中占有非常重要的地位。下面详细叙述 Active Directory 的相关内容。

(1) Active Directory 的逻辑结构

Active Directory 在逻辑上由对象、组织单元、域、域树和域林构成层次结构。这种逻辑层次结构类似于树型结构，是由下而上建立的。首先是一个单一的域，为了管理方便，划分了许多组织单位，形成一个个的分支结构，活动目录为每个域建立一个目录数据库的副本，这个副本只能存储用于这个域的对象。

当组织单元或其中的对象很庞大，又可划分为许多更小的域时，这些有相互关系的域组成一棵域树。每棵域树中，每个域都拥有自己的目录数据库副本，存储自己的对象，并且可以查找域树中其他的目录数据库的副本。如果再将域树组合，则可构成域林。

① 对象

对象(Object)是活动目录组织的基本单元，可以是用户、计算机、文件以及打印机等网络资源。对象是对象类的一个实例，而每个对象类有很多属性，如名字、邮箱、地址等。这些属性被封装在对象内部，提高了对象安全性，并且便于组织、管理和控制对它的访问。每个对象必须有一个全域唯一的标识名，这个标识名被称为 DN。

② 组织单元

组织单元(Organizational Units，OU)是组织、管理一个域内的对象的容器，它可以包括用户、组、计算机和其他组织单位，但是组织单元不能包括来自其他域的对象。组织单元具有很清晰的层次结构。这种层次结构可以使管理者把组织单元放到域中，以反映出整个域的组织结构，并且可以委派任务与授权。

③ 域

域(Domain)是由集中共享账户数据库管理的用户和计算机组成的逻辑分组。域的最大的优点是单一网络登录能力，即用户只要在域中有一个合法的账号，登录到域后就可以访问域中对该用户授权许可的共享资源。在域内，密码和权限很容易标示，因为域里有一个包括用户账户、权限和其他网络细节信息的中心数据库，此数据库的信息可以在域控制器之间自动复制。域必须有域控制器，它控制着用户的认证，只有得到认证的用户才能顺利登录域，登录之后才可以在规定的权限内使用域内资源。

④ 域树

将多个域合并而成为一个有层次排列的新的集合称为域树(Domain Tree)。域树形成一个连续的域名空间(域名空间指的是任何拥有相同 DNS 根名的域的集合)，共享同一表结构和配置。域树中第一个域称为根域，同一域树的其他域为子域。同一域树中，紧接在域上面的域，是子域的父域。活动目录包含一个或多个域树。域树中的域层次越深级别越低，一个“.”代表一个层次。如图 6-2 所示，域 www. xyz. com 就比 xyz. com 域级别低，因为它有两个层次关系。

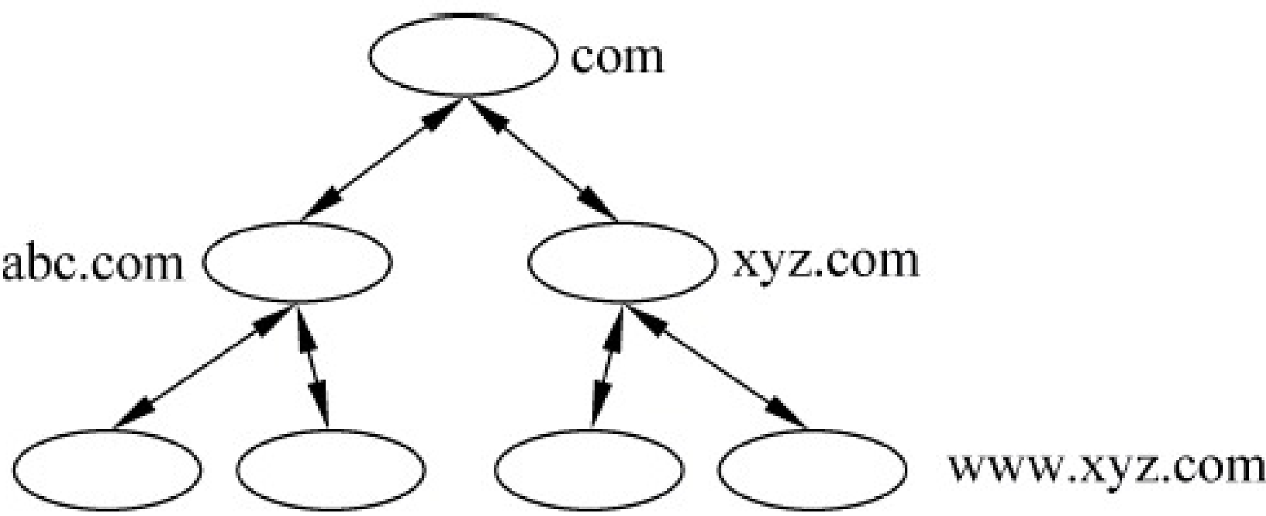


图 6-2　域树的层次

⑤ 域林（Forest）

由一个或多个没有形成连续域名空间的域树组成的逻辑关系，称为域林。与域树最明显的区别是，域林中的所有域树之间没有形成连续的域名空间，域林中的所有树都具有相同的架构、配置和全局编录。在域林中创建的第一棵域树被默认为该域林的根树。当域林建立起来时，每一棵域树的根域会自动建立双向的信任关系。所以，每一个域的使用者只要有足够的权限，就可以访问其他域树的资源。如图 6-3 显示了一个域林的结构。

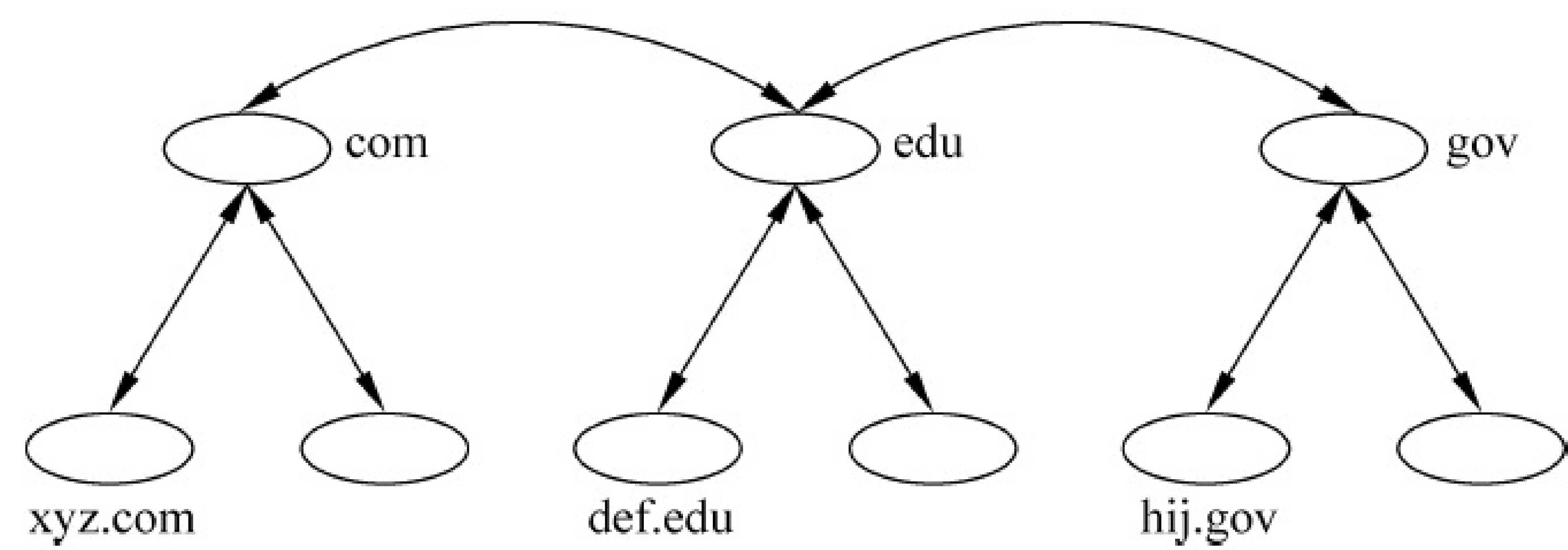


图 6-3　域林的结构

（2）Windows Server 2003 在网络中的三种角色

根据不同的需要，Windows Server 2003 在网络中可以充当域控制器、成员服务器和独立服务器三种角色。

① 域控制器

域控制器是安装活动目录的计算机。域控制器主要负责管理用户对网络的各种访问权限，包括登录网络、账户的身份验证以及访问目录和共享资源等。当一个网络中只存在一台 Windows Server 2003 服务器时，一般要将其设置为域控制器。

② 成员服务器

成员服务器不能作为独立的服务器，只能是域的成员。它不处理域账户有关的信息，不需安装活动目录，也不存储与系统安全策略有关的信息。但是，在成员服务器上也可以为用户或组设置访问权限，允许用户连接到该服务器并使用相应的资源。成员服务器主要用于以下类型的服务器：文件服务器、应用程序服务器、数据库服务器、Web 服务器、证书服务器、防火墙和远程访问服务器等。

③ 独立服务器

独立服务器是指运行 Windows Server 2003 操作系统，但不作为域成员的计算机，也就是说它是一台具有独立操作功能的计算机。在此计算机上不再提供其他用户的账户信息，也不提供登录网络的身份验证等工作。独立服务器能以工作组的形式与其他计算机组建对等网，在访问其他计算机时，也可以将自己的资源提供给其他计算机访问。

使用活动目录安装向导，可将成员服务器升级为域控制器，也可以将域控制器降级为成员服务器或独立服务器。

（3）安装 Active Directory

要将 Windows Server 2003 的网络设置为域结构，则网络上必须有域控制器。域控制器通过 Active Directory 提供目录服务，例如负责管理 Active Directory 计算机资源、审核用户的账户与密码等。在默认安装 Windows Server 2003 时，系统并不会自动安装

Active Directory,若网络中没有域控制器,则可将该独立服务器或成员服务器配置为新域的域控制器;若网络中有其他域控制器,可将其配置为额外域控制器。

① 当独立服务器或成员服务器重新启动时,以系统管理员的身份登录,执行菜单命令"开始"→"程序"→"管理工具"→"配置服务器",打开如图 6-4 所示的"配置您的服务器向导"对话框。也可以在运行对话框中执行"dcpromo"启动"配置您的服务器向导"对话框。

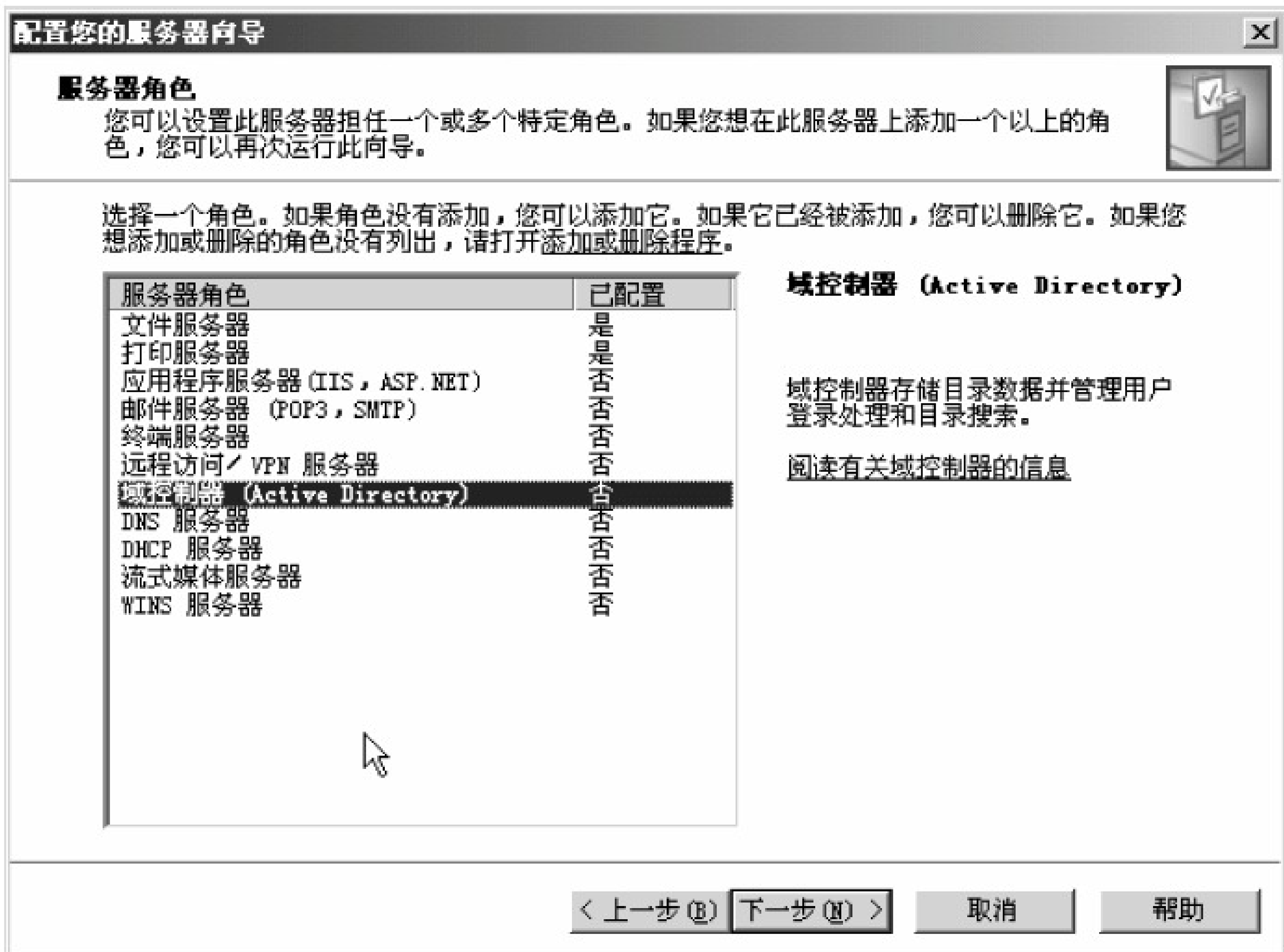


图 6-4　启动 Active Directory 向导

单击左边的"域控制器"(Active Directory),选择下方的"启动 Active Directory 向导",单击"下一步"按钮。

② 在如图 6-5 所示的"域控制器类型"界面中选择"新域的域控制器"单选按钮,使服务器成为新域中的第一个域控制器,然后单击"下一步"按钮。

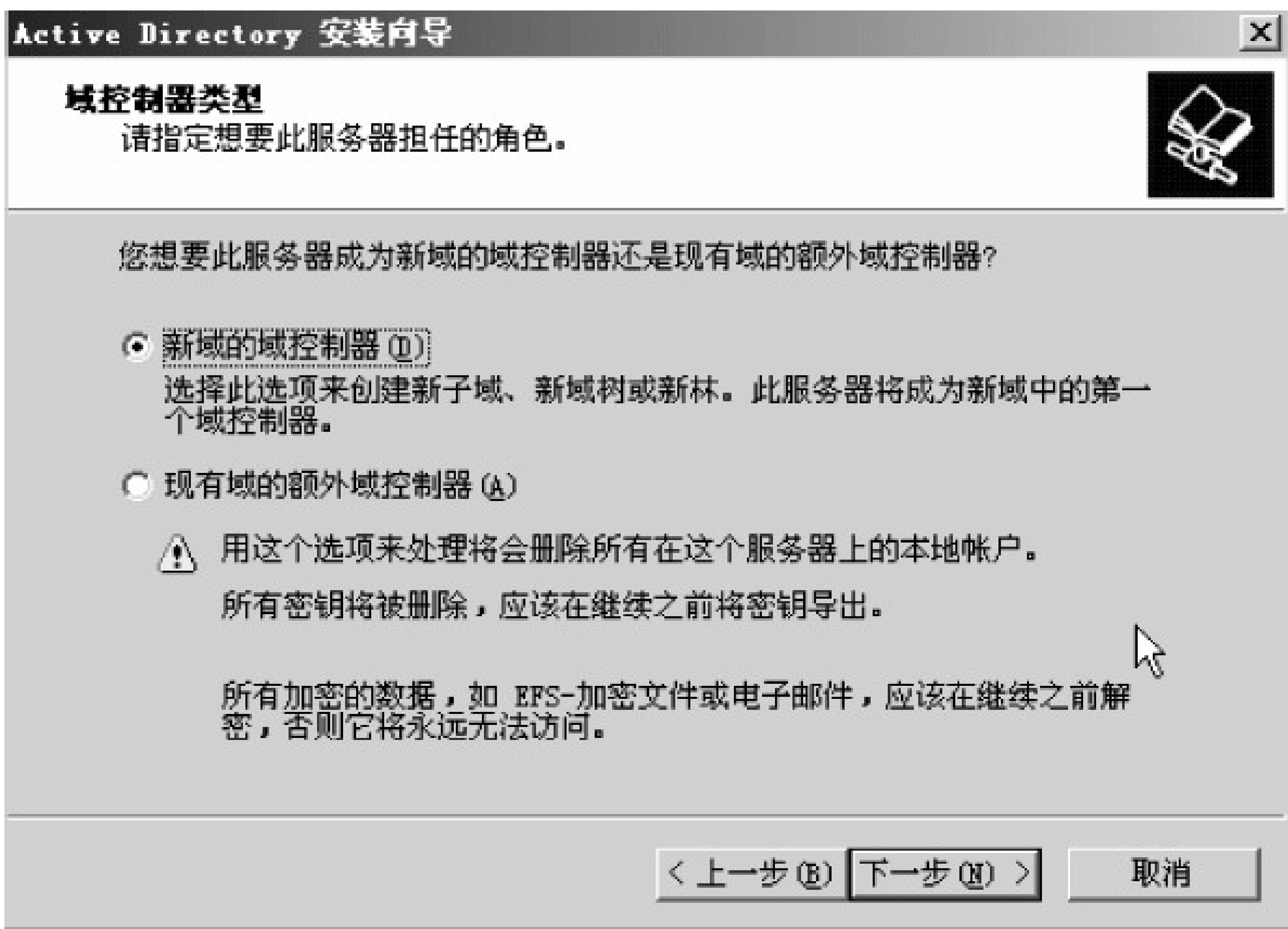


图 6-5　选择域控制器类型

③ 在如图 6-6 所示的界面中选择"在新林中的域"单选按钮,然后单击"下一步"按钮。打开如图 6-7 所示的"新的域名"对话框,在"新域的 DNS 全名"文本框中,输入在

Internet 命名机构注册的新域的 DNS 全名，例如 sdcit. com；单击“下一步”按钮。在如图 6-8 所示的“NetBIOS 域名”对话框的“域 NetBIOS 名”文本框中，输入 NetBIOS 新名称，该名字可以让早期的 Windows 版本来识别新域，然后再单击“下一步”按钮。

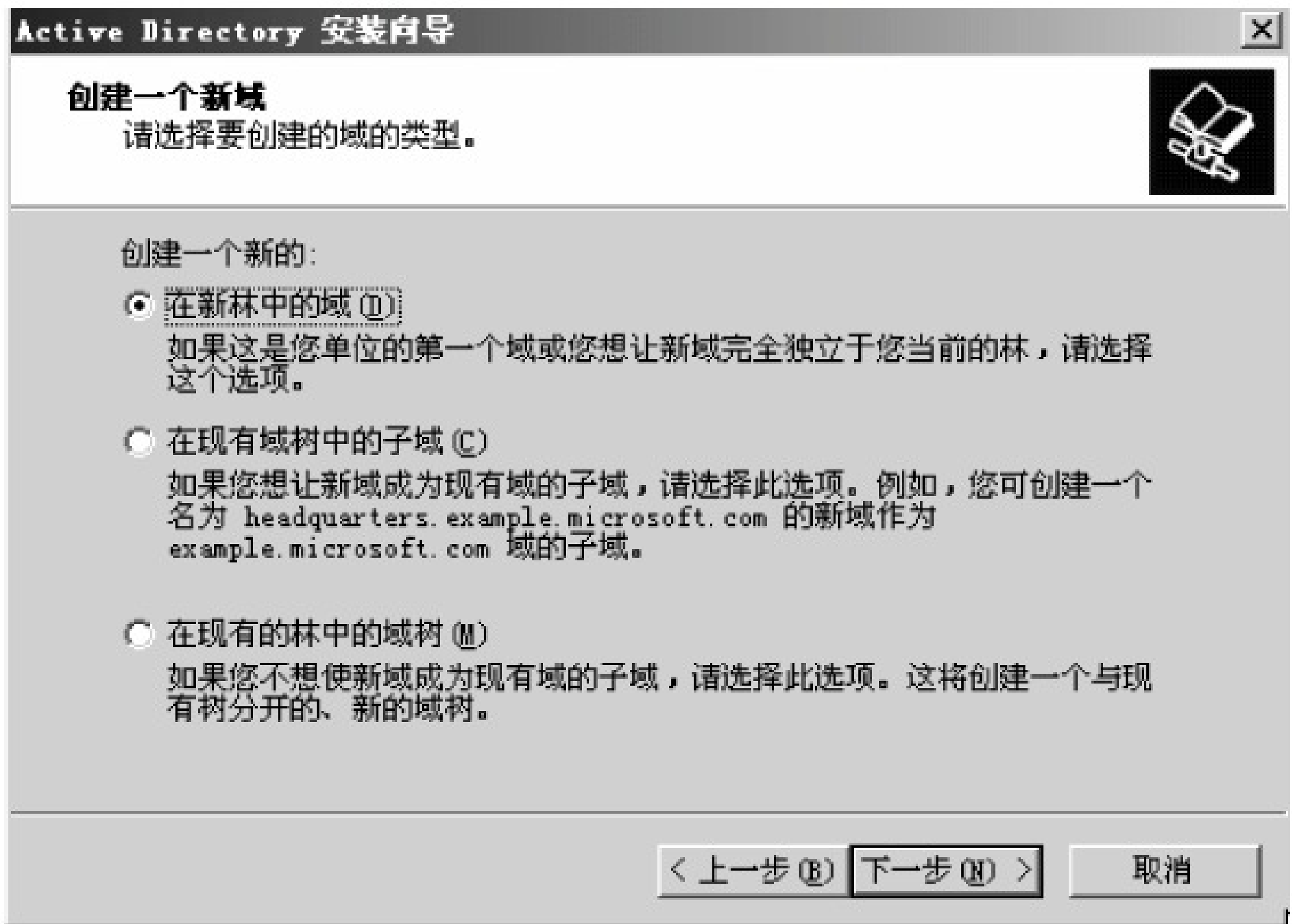


图 6-6　创建目录树或子域



图 6-7　指定新域名

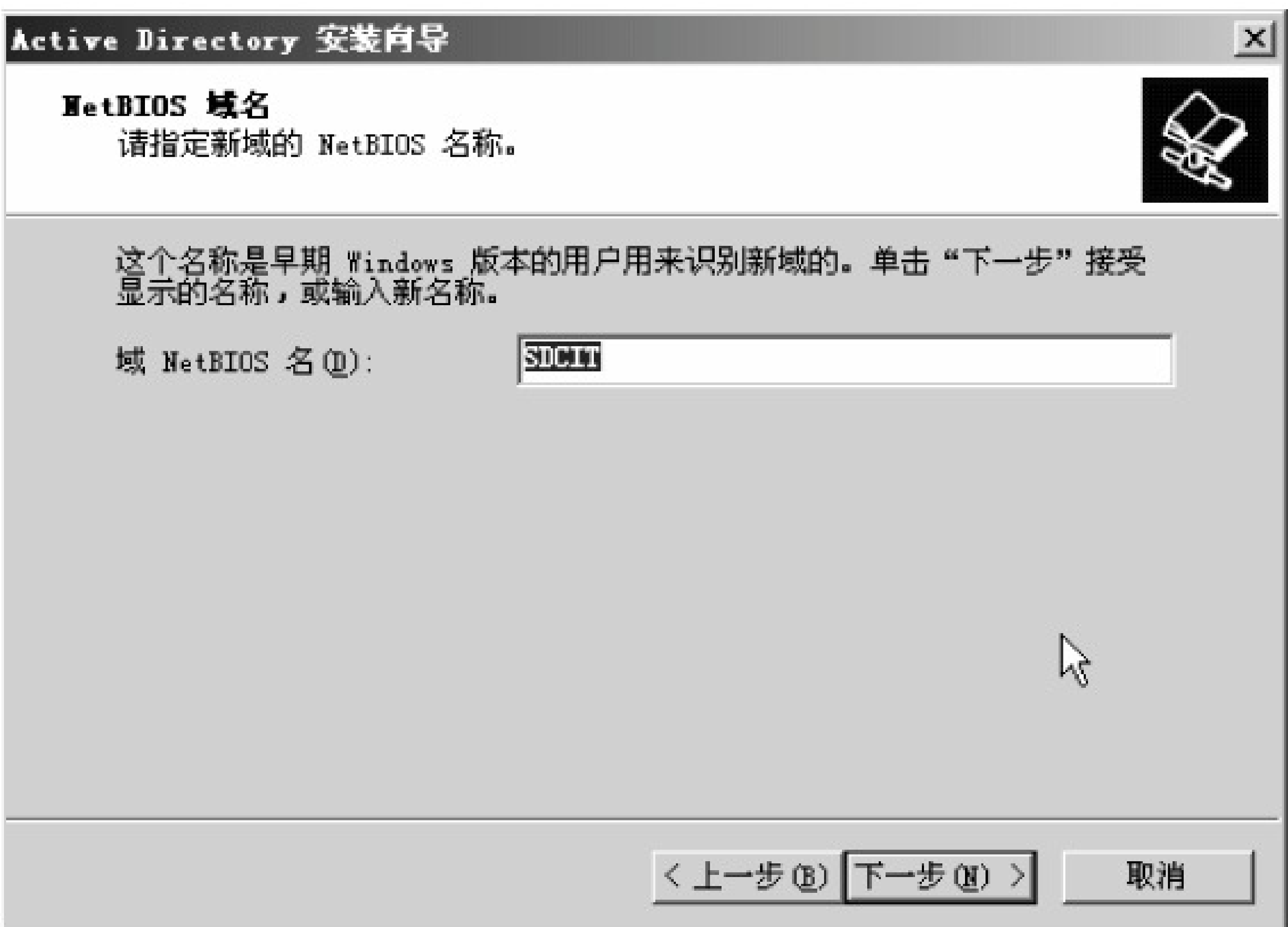


图 6-8　输入 NetBIOS 域名

④ 打开“数据库和日志文件位置”对话框，在“数据库位置”文本框中设置保存活动目录数据库的位置；在“日志位置”文本框中设置保存日志的位置。尽可能设置到不同的硬盘上，以提高安全性和性能。然后单击“下一步”按钮，如图 6-9 所示。

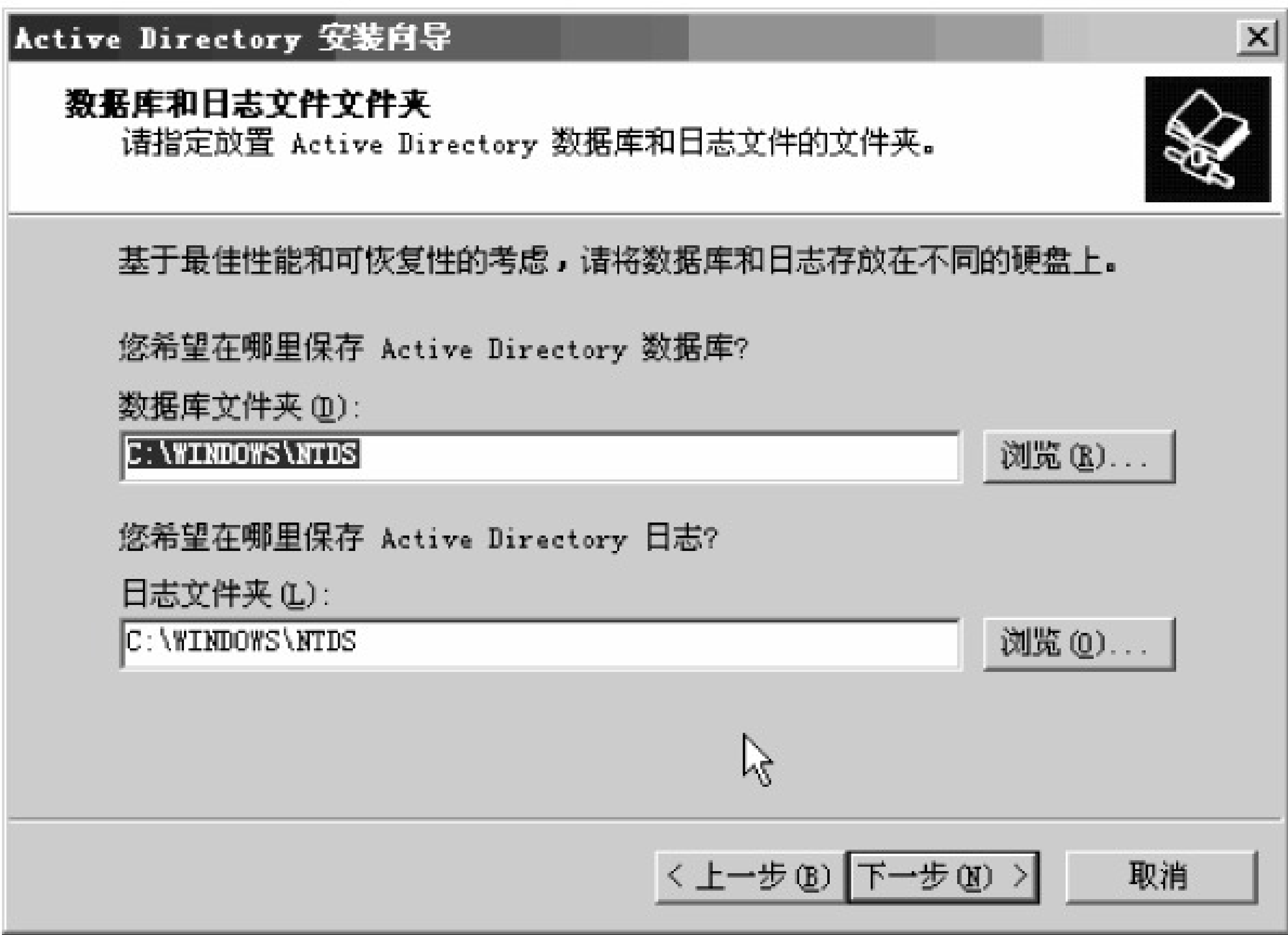


图 6-9　指定数据库和日志文件的位置

⑤ 打开如图 6-10 所示的“共享的系统卷”对话框，在“文件夹位置”框中设置 SYSVOL 文件夹的位置，要求该文件夹必须存放在 NTFS 卷上。单击“下一步”按钮。在 Windows Server 2003 中，SYSVOL 文件夹存放域的公用文件的服务器副本，它的内容将被复制到域中的所有域控制器上。

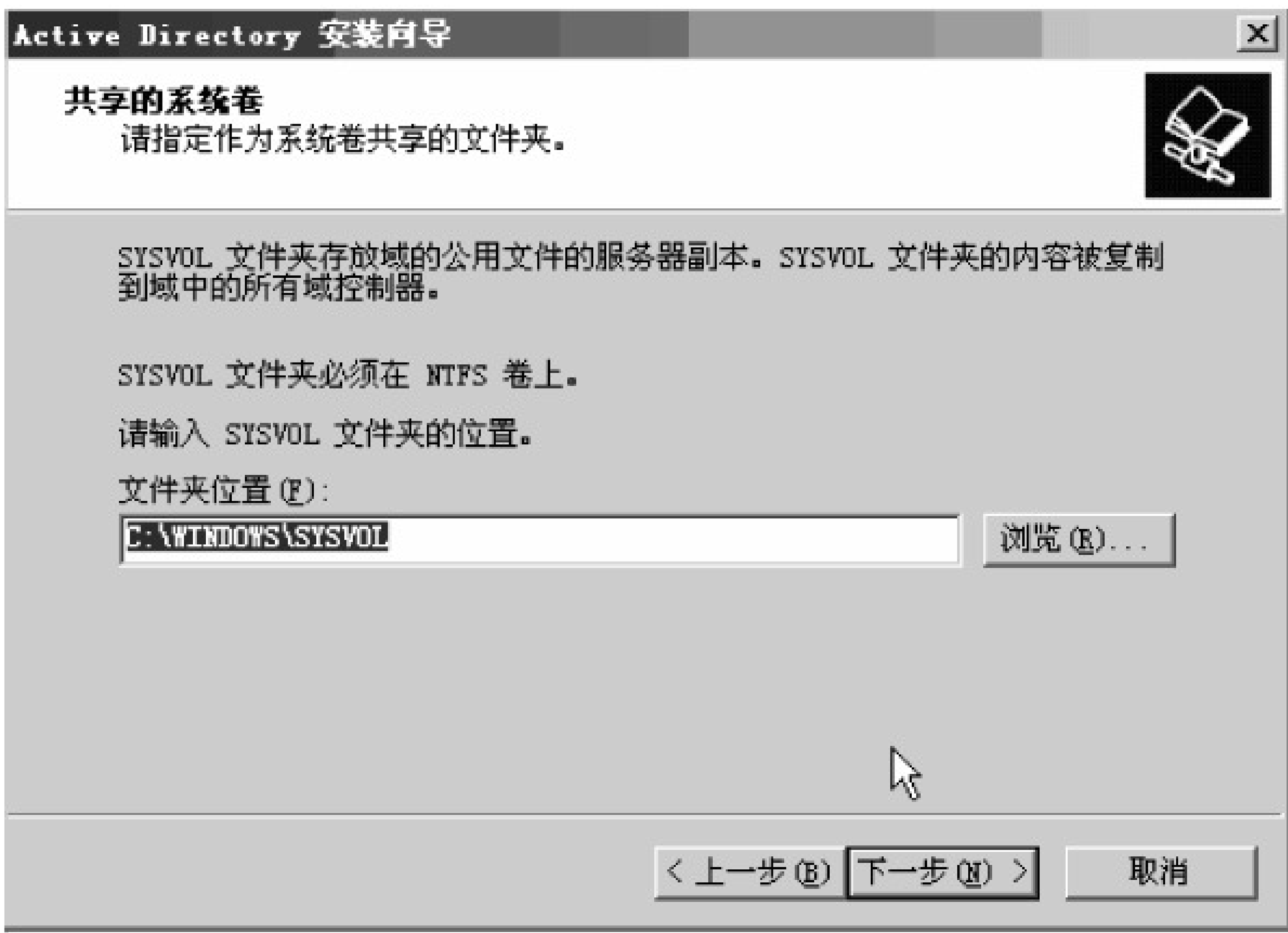


图 6-10　指定系统卷共享的文件夹的位置

⑥ 系统将自动检测是否安装或注册了 DNS 服务器，若没有配置，则提示用户配置 DNS 服务器，如图 6-11 所示。在这里，选择“在这台计算机上安装并配置 DNS 服务器，并将这台 DNS 服务器设为这台计算机的首选 DNS 服务器”单选按钮，然后单击“下一步”按钮。

⑦ 在如图 6-12 所示的对话框中，选择“与 Windows 2000 之前的服务器操作系统兼容的权限”或“只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限”单选按钮。然后单击“下一步”按钮。

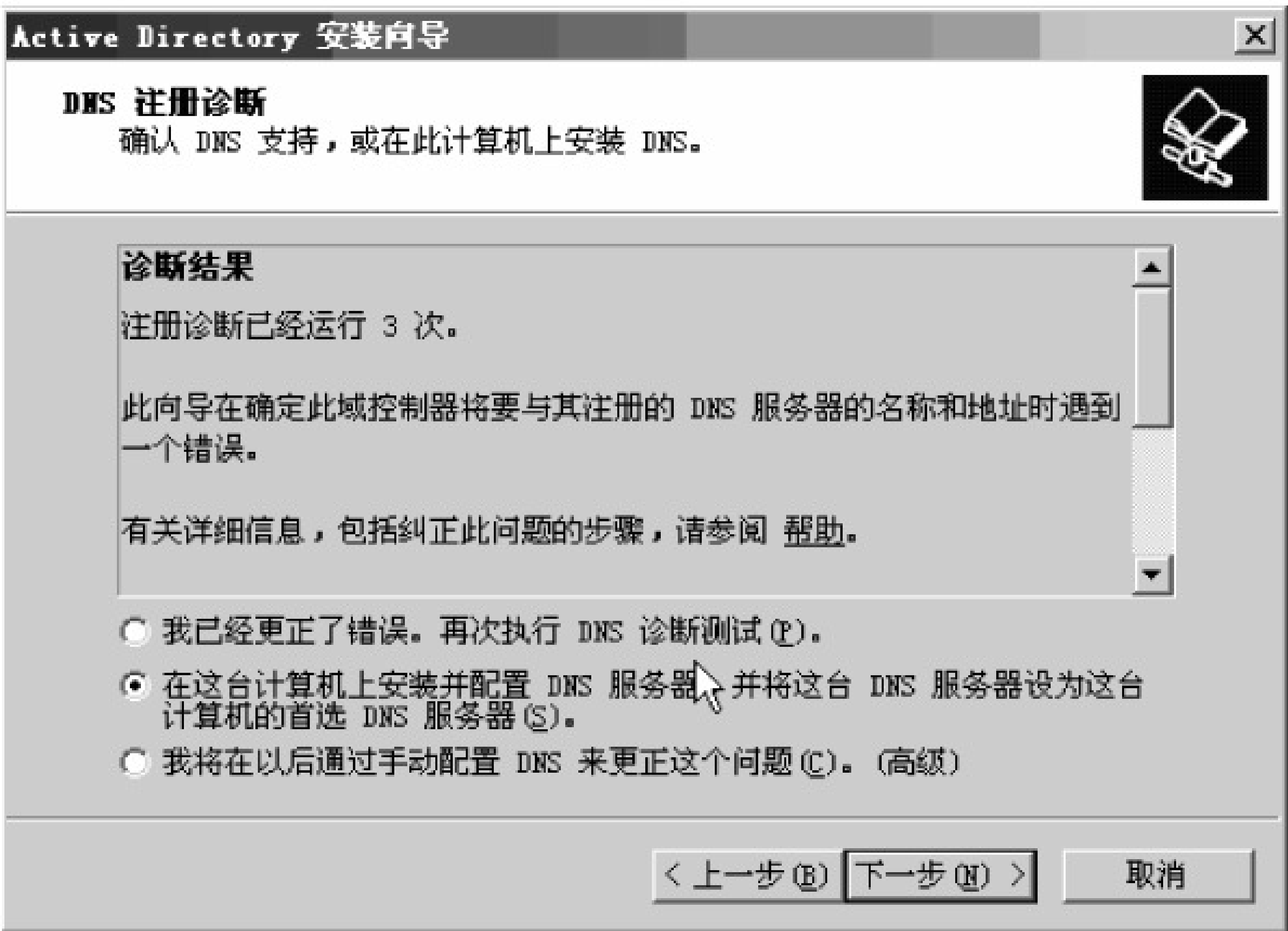


图 6-11　DNS 注册诊断

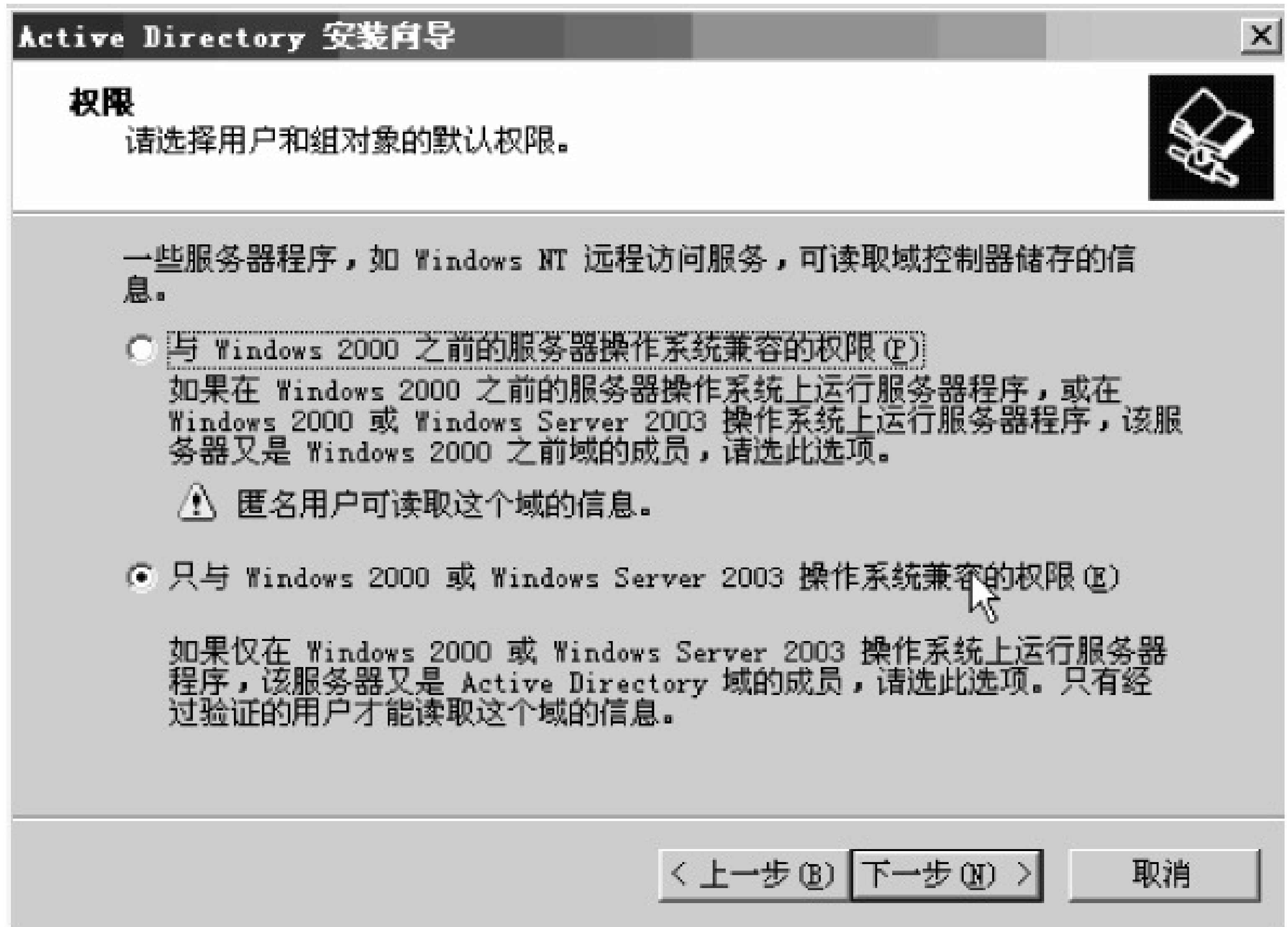


图 6-12　为用户和组对象选择默认权限

⑧ 在如图 6-13 所示的“目录服务还原模式的管理员密码”对话框中，输入用于修复目录服务的密码，单击“下一步”按钮。

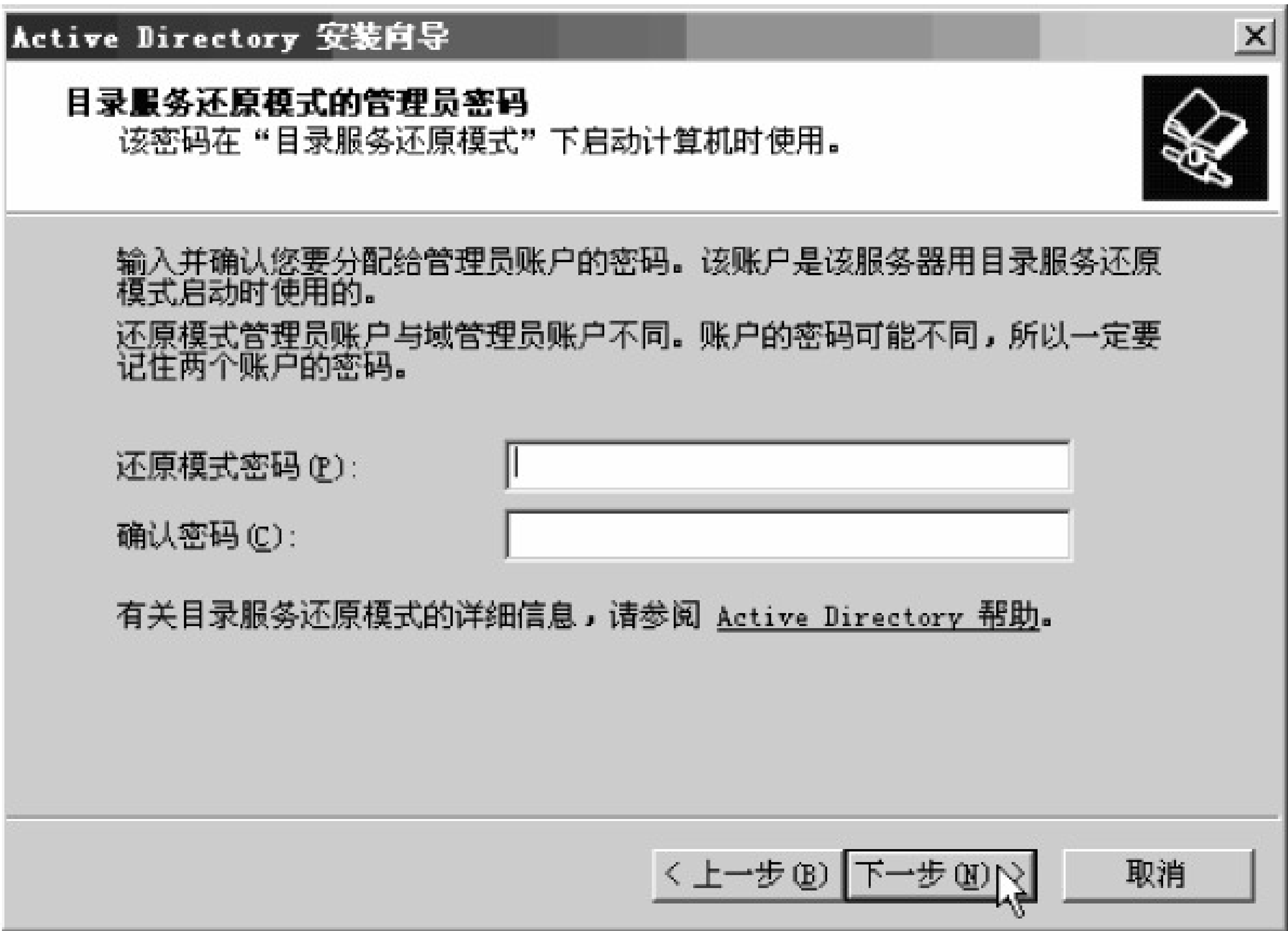


图 6-13　设置目录服务恢复模式的管理员密码

⑨ 打开如图 6-14 所示的“摘要”对话框，用户可检查设置的选项。然后单击“下一步”按钮。

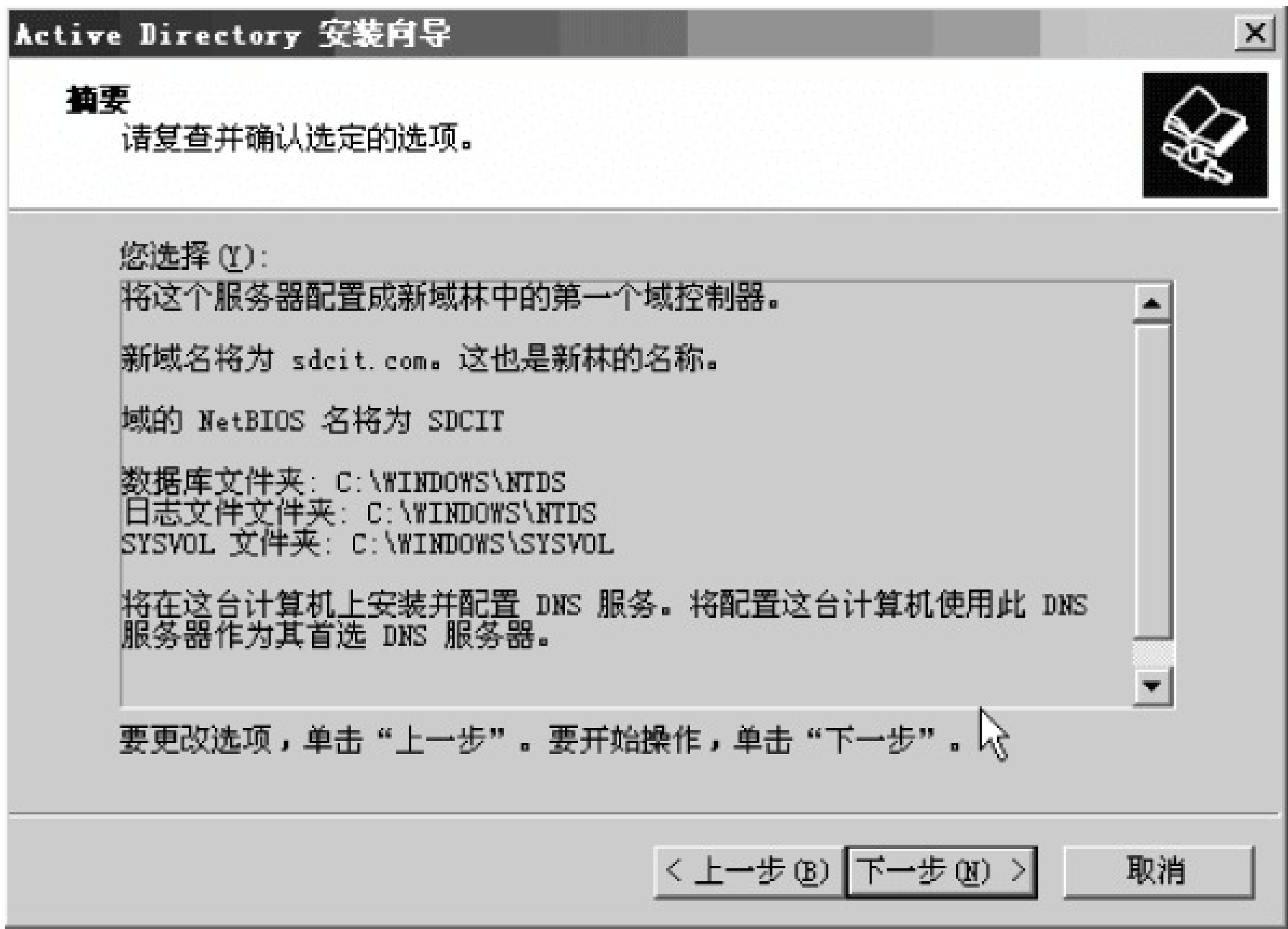


图 6-14 “摘要”对话框

⑩ 系统开始配置 Active Directory，同时打开“正在配置 Active Directory”对话框，提示配置过程。Active Directory 配置完成后，单击“完成”按钮。这样重新启动计算机后，Active Directory 开始起作用。

6.1.5 Windows Server 2003 用户与组的管理

任务描述：在一个网络环境中共有 3 台计算机，用 C1、C2、C3 表示，使用的操作系统是 Windows Server 2003；用户用 U1、U2、U3 表示。实现用户之间的资源共享和信息传递。

任务分解：当用户 U2、U3 要使用计算机 C1 上的资源时，必须由 C1 的管理员 U1 完成指定 U2、U3 在本地计算机上的设置。如果计算机的用户有成千上万个，每个用户的权限都要由管理员去设置的话，那么管理员管理起来是相当麻烦的。为此使用域管理用户是非常方便的。

1. 用户账户介绍

(1) 本地用户账户

本地用户账户是在本地计算机上建立的用户账户。只允许用户使用本地资源。

(2) 域用户账户

域用户账户是指在域中创建的账户，该账户信息存放于域控制器的目录数据库中，并且在其他的域控制器中备份。这样在域中的任意一台计算机上登录，都能使用该域中的资源，其权限要比本地用户账户的权限大。

2. 用户账户的创立和管理

要实现对用户账户的管理，首先从计算机中依次单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口。

(1) 创建新的用户账户

① 在“Active Directory 用户和计算机”窗口左侧的目录树中找到域节点，双击打开。

② 右击欲创建的新的用户账户的组织单位或容器，在弹出的快捷菜单中选择“新建”→“用户”命令。或选中“Users”文件夹，单击“Active Directory 用户和计算机”窗口中菜单栏上的“创建用户”图标，打开“新建对象-用户”对话框，如图 6-15 所示。

③ 在“姓”和“名”文本框中，输入姓氏和名字，在“用户登录名”文本框中输入用户登录名。

注意：*系统中的用户名是唯一的，不能和其他用户重名，且用户名不超过 20 个字符。用户名可以包含大小写字母、数字和中文，但不能包含小数点和空格。用户名是区分字母的大小写的。*

④ 单击“下一步”按钮，进入密码输入对话框，如图 6-16 所示。



图 6-15　新建用户



图 6-16　设置密码

⑤ 输入密码和确认密码并根据用户的属性选择合适的复选框后，单击“下一步”按钮，出现“新建对象-用户”对话框，如图 6-17 所示。

⑥ 确认上述所创建的用户信息无误后，单击“完成”按钮即可，否则依次单击“上一步”按钮，返回上一步骤，对创建的信息进行修改。

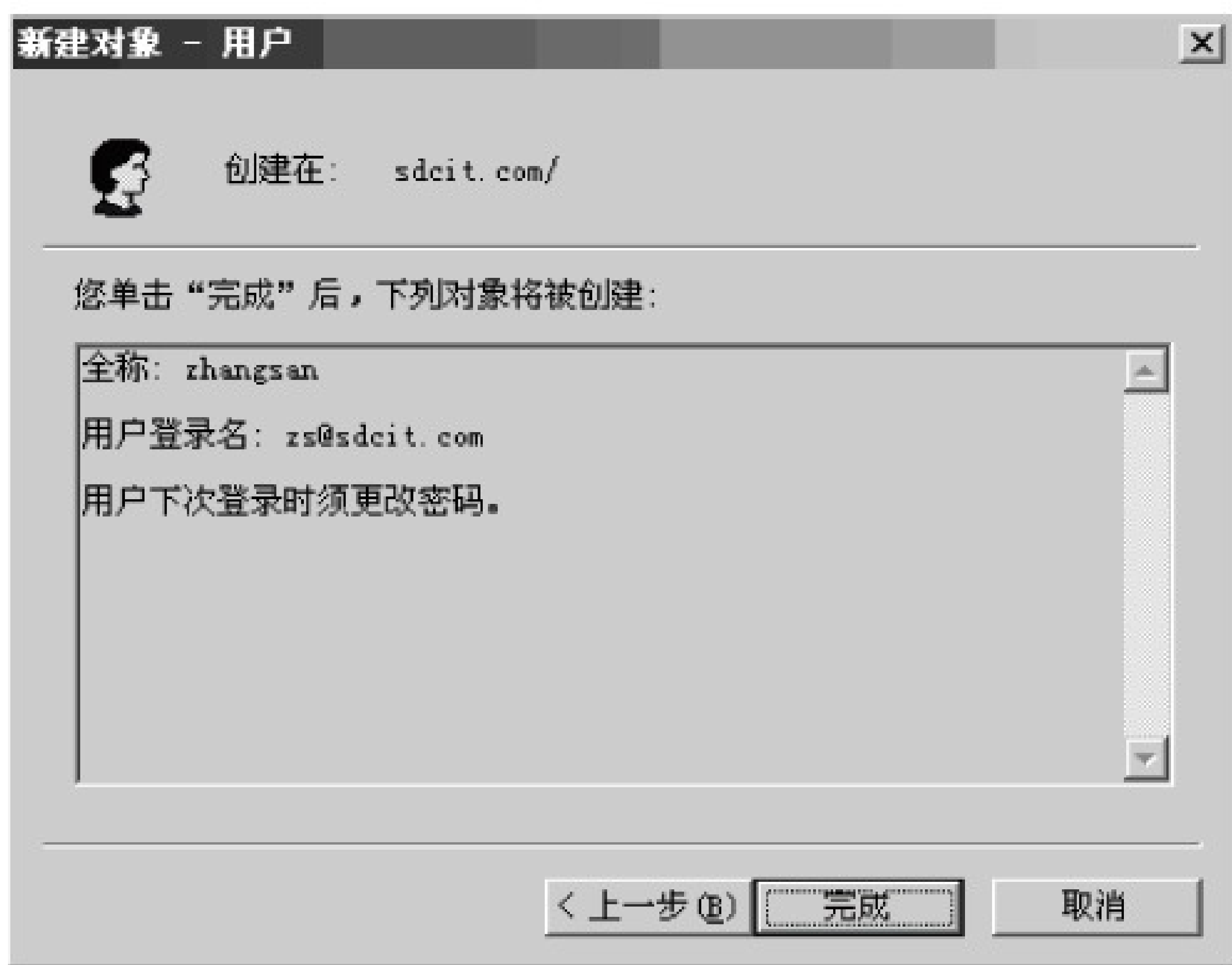


图 6-17　完成对话框

新用户创建完成后，在用户窗口中就会出现新建的账户及其所隶属的组。能够看到对于任何一个新账户，其默认的组都是“Users”组。

(2) 删除用户

在控制台左侧窗口中，单击展开域节点，右击想要删除的账户，从弹出的快捷菜单中选择“删除”命令，经过确认信息后即可。

(3) 账户属性设置

右击选中的用户账户，从弹出的快捷

菜单中选择“属性”命令，打开“属性”对话框，单击“账户”属性页即可。该页还包括以下几点。

- 登录时间：确定用户登录到域的时间。
- 登录到：选择用户登录的站点。
- 账户选项：对用户的密码属性做出修改。
- 账户过期：限制用户账户的使用时间。

（4）管理用户账户

要想管理一个用户账户，右击选中该账户，从弹出的快捷菜单中选择相应的操作即可，主要有：

- 添加到组：设置用户所属的组。
- 禁用账户：停止该用户的使用。
- 重设密码：重新设置用户的密码。
- 复制：想建立多个相同属性的用户账户时，可以使用“复制”命令。
- 移动：将该账户移动到另外的容器中。
- 重命名：更改用户账户的名称，其中的属性不会发生变化。

（5）设置用户的配置文件

若用户要在不同的计算机上登录到域，并能方便地连接到自己在文件服务器上的文件夹。操作步骤如下：

① 在文件服务器上创建一个共享文件夹，设置共享名，如 wyj，并设置共享权限。

② 在用户账户的属性对话框中，打开“配置文件”选项卡。

③ 在“主文件夹”区域中，选择“连接”项，选择驱动器号，如 M：。输入用户主文件夹的网络路径，如\\192.168.10.3\wyj\LL。

设置完成后系统会自动在共享文件夹 wyj 中建立一个名为 LL 的子文件夹。若在 NTFS 分区，还会自动设置相应的 NTFS 权限，保证只有该账户可以访问该文件夹。

这样设置后就可以在任何一台机器的“我的电脑”中看到自己文件夹影射的网络驱动器，可以方便地访问自己的主文件夹。

3. 组的管理

在大型的网络系统中，由于用户账户很多，分别设置权限非常复杂。而且有很多用户账户具有相同的权限，这样可以把相同属性的用户账户划归到用户组中，利用组的特性，简化对网络中的资源访问的管理。

将一个用户账户添加到组后，该账户就拥有该组的一切权限，一个用户可以是多个组的成员。

（1）组的作用域

组的作用域是指在域树或域林中所应用的范围。包括：本地域组、全局组和通用组。

本地域组：该作用域仅适于本身所在域的主控制器、成员服务器和域工作站，不能跨越域。利用该作用域为域中的资源分配相应的权限。

全局组：该作用域仅适于本身所在域的主控制器、成员服务器和域工作站和其他被信任的关系域。利用该作用域来组织有类似网络资源需求的用户。

通用组：指定给多个域中的相关资源的授予权限。可以来自任何域。在所有相连的域中都有效。

（2）组的类型

安全组：具有对对象和资源使用的访问权限，也可以作为电子邮件实体。域账户都属于某个安全组。

分布式组：又称为通信组，只能适用于电子邮件实体，无法设置该组的权限。

（3）内置组

根据实际的需要，将内置的使用权力分配给用户，使这些用户都具有该域的管理权限。内置的本地域组只能在域控制器上，不能删除。系统默认情况下建立了以下内建全局组：

① Domain Admins

该组可以代表具有操作域权力的用户。通常情况下，Domain Admins 属于 Administrators 组，因此该组的成员可以在域中执行管理工作。因此，如果希望某一用户成为域系统管理者，则最好将该用户加至 Domain Admins 组中，而不要直接加至 Administrators 组中。

② Domain Guests

所有域来宾的组，Windows Server 2003 系统会自动将 Guest 用户账户加至该组，并将该组加至内建本地域 Guests 组中。

③ Domain Users

所有域的成员的组，在预设的情况下，任何我们所建立的用户账户都会是 Domain Users 组的成员，而任何所建立的计算机账户又都会是 Domain Computers 组成员。因此如果我们想要让所有的账户都具有某种资源存取权限，则可以将该权限指定给 Domain Users 组或让 Domain Users 组属于具有该权限的组。

④ Enterprise Admins

提供授权具有管理整个网络权力用户的方法。

（4）组的管理

① 组创建。包括组名、组类型、组作用域。

② 更改组作用域。只有域为本机模式时，才能起作用。

③ 删除组。组被删除其相应的权限也被一起删除，但是该组的成员账户或组不能删除。

④ 添加成员。可以包括用户账户、计算机、其他组。

⑤ 添加到组。组可以添加到其他组中，作为其他组的成员。

4. 组织单位的管理

（1）创建组织单位

在域控制器中打开“Active Directory 用户和计算机”窗口，右击域名，选择“新建”项，选择“组织单位”命令；输入组织单位名称，单击“确定”按钮；将组织单位内包含的账户、计算机、共享资源等移动到组织单位中进行管理。

（2）组织单位的委派控制

组织单位委派是指将组织单位的某些管理权限赋予一个或多个指定用户，以方便管理。步骤如下：右击所建立的组织单位，选择“委派控制”项；单击“添加”按钮，选择要添

加的用户,单击“下一步”按钮;选择要将组织单位的哪些管理权限委派给该用户。

5. 在域中创建计算机账户

(1) 将成员服务器加入域中

以安装了 Windows Server 2003 的计算机为例,将其加入到域中,成为域中的成员服务器。

① 启动成员服务器,在该服务器的桌面上右击“我的计算机”,在弹出菜单中选择“计算机名”选项。

② 单击“更改”按钮,弹出“计算机名称更改”对话框,选择隶属于“域”,输入要加入的域名称。

③ 单击“确定”按钮,弹出“域用户名和密码”设置对话框,输入该域中合法的账户名称和密码。

④ 单击“确定”按钮,弹出“网络标识”对话框,单击“确定”按钮后重新启动计算机即可。

(2) 将客户端计算机加入域中

以安装了 Windows XP 的计算机为例,将其加入到域中。

① 在客户端计算机的桌面上右击“我的电脑”,在弹出菜单中选择“计算机名”选项。

② 单击“更改”按钮,弹出“计算机名称更改”对话框,选择隶属于“域”,在里面写上要加入的域名称。

③ 单击“确定”按钮,弹出“域用户名和密码”设置对话框,输入该域中合法的账户名称和密码。

注意:输入的该域的账户和密码必须是已经在域控制器中注册好的用户和密码,否则不能加入到该域中。

④ 单击“确定”按钮,弹出“网络标识”对话框,单击“确定”后重新启动计算机即可。

6.1.6 共享文件夹

任务描述:学院各个部门在文件服务器上都有自己的文件夹。要求:①全院职工都可以访问到人事处文件夹下的子文件夹“通讯录”;②财务审计处的职工可以访问人事处文件夹下的职工考勤子文件夹,和教务科研处的教师工作量文件夹;③财务审计处的工资文件夹内容只能被王老师修改;④院长能看所有部门文件夹的所有内容。

任务分解:完成本任务,需要首先了解文件在计算机中的存储形式属性。这涉及文件系统、NTFS 权限类型、NTFS 权限设置、NTFS 权限规则、共享文件夹等概念。

1. 文件系统

文件系统是对文件组织和管理的方式。Windows Server 2003 主要支持 FAT16、FAT32、NTFS 三种文件系统。从安全角度考虑,计算机网络服务器一般采用 NTFS。

NTFS 文件系统能够管理较大的卷,是一个可恢复的文件系统。NTFS 支持对分区、文件夹、文件的压缩,并且对压缩文件读取不需要事先解压缩,文件关闭和保存会自动压缩;可以限制用户使用磁盘的大小等。

NTFS最主要的特点是安全性能方面。在NTFS分区上,可以为共享资源、文件夹以及文件设置访问许可权限,包括哪些用户可以访问和访问的权限大小;访问许可权限对本地用户和网络用户一样都起作用;NTFS中的审核策略可以查看用户进行了什么样的操作。

在不破坏原有数据的情况下可以使用命令将FAT32文件系统的分区转换为NTFS分区。格式例如:convert e:/fs:ntfs。

2. NTFS权限类型

系统管理员和文件拥有者可以指定特定用户和组对某个文件或文件夹的权限,实现对资源的保护。

(1) 文件夹的NTFS权限

用来控制用户对文件夹和其下的文件及子文件夹的访问。包括以下几种。

① 列出文件夹目录。允许查看文件夹内包括的内容,但不能打开其中的文件;允许看文件夹的属性、权限设置、所有者等。

② 读取。可以打开文件夹中的数据文件。

③ 读取和执行。可以打开文件夹中的应用程序文件。

④ 写入。允许创建新文件和子文件夹,改变文件夹属性,查看权限和所有者。

⑤ 修改。具有"写入"、"读取和执行"的权限;可以删除文件夹和文件。

⑥ 完全控制。允许全部的权限,可以更改文件夹的NTFS权限,可以获取文件夹的所有权。

(2) 文件的NTFS权限

用来控制用户对文件的访问。包括以下几种。

① 读取。允许查看文件内容、所有者、属性和权限。

② 读取和运行。可以运行应用程序。

③ 写入。改写文件、更改文件属性以及查看所有者和权限。

④ 修改。具有"读取和运行"、"写入"的权限,允许修改和删除文件。

⑤ 完全控制。可以获得文件的所有权。

(3) NTFS权限的规则

① 子文件夹和文件默认继承父文件夹的权限;用户及其所属组的权限。

② 文件权限优先于文件夹权限。

③ 拒绝权限优先于允许权限。

④ 在同一分区上复制,继承目标文件夹的权限;移动、保留原权限。

⑤ 不同分区上复制和移动,都会继承目标文件夹的权限。

⑥ 将文件从NTFS分区移动或复制到FAT分区,所有的NTFS权限设置丢失。

3. NTFS权限设置

NTFS权限设置只有拥有者,具有完全控制权的用户和系统管理员才可以设置。

(1) 设置文件夹的NTFS权限

右击目标文件夹(在NTFS分区上),打开"属性"对话框;打开"安全"选项卡,单击"高级"按钮;取消"允许父项的继承权限传播到该对象和所有资源对象"复选框的选择,

单击“复制”按钮，将原来的权限保留到该对象；删除不需要对文件夹具有权限的用户和用户组；单击“添加”按钮，添加要对文件夹操作的账户并选择允许和拒绝的权限；单击“确定”按钮，设置完的窗口如图 6-18 所示。



图 6-18　高级安全设置

（2）设置文件的 NTFS 权限

设置文件的 NTFS 权限的方法和文件夹的 NTFS 权限的设置方法相同。

（3）NTFS 特殊权限

特殊权限是对标准权限的细化，标准权限可以看做特殊权限的特定组合。如允许用户在文件夹中创建文件，但不能创建文件夹，这样必须设置用户的 NTFS 特殊权限。

特殊权限的设置方法：打开“安全”选项卡，单击“高级”按钮；选择要设定特殊权限的用户；单击“编辑”按钮，进行详细的设置。

NTFS 特殊权限包括：遍历文件夹/运行文件、列出文件夹/读取数据、读取属性、读取扩展属性、创建文件/写入数据、创建文件夹/附加数据、写入属性、写入扩展属性、删除文件夹及文件、删除读取权限、更改权限、取得所有权等。如图 6-19 所示。

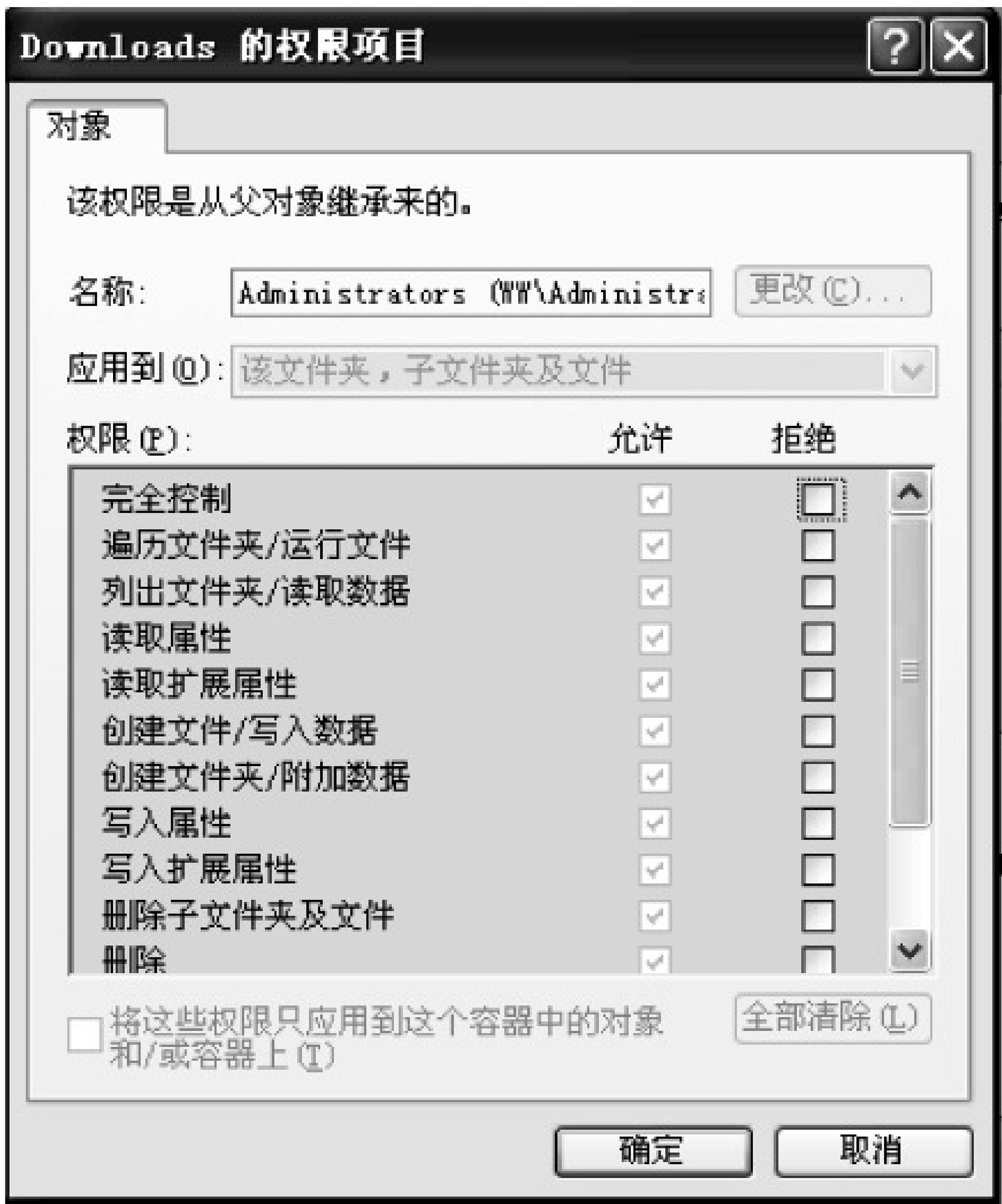


图 6-19　权限项目选择

（4）对象的所有权

对象的所有者与其他权限是彻底分开的。对象的所有者具有更改对象的权限设置的能力。

Administrators 组的成员可以取得系统中任意对象的所有权。取得所有权的方法如下。

打开对应文件夹的属性对话框,打开“安全”选项卡,在出现的提示信息中,单击“确定”按钮;在“安全”选项卡中,单击“高级”按钮,打开“所有者”选项卡,选择将所有者改为对应的用户,如图 6-20 所示。

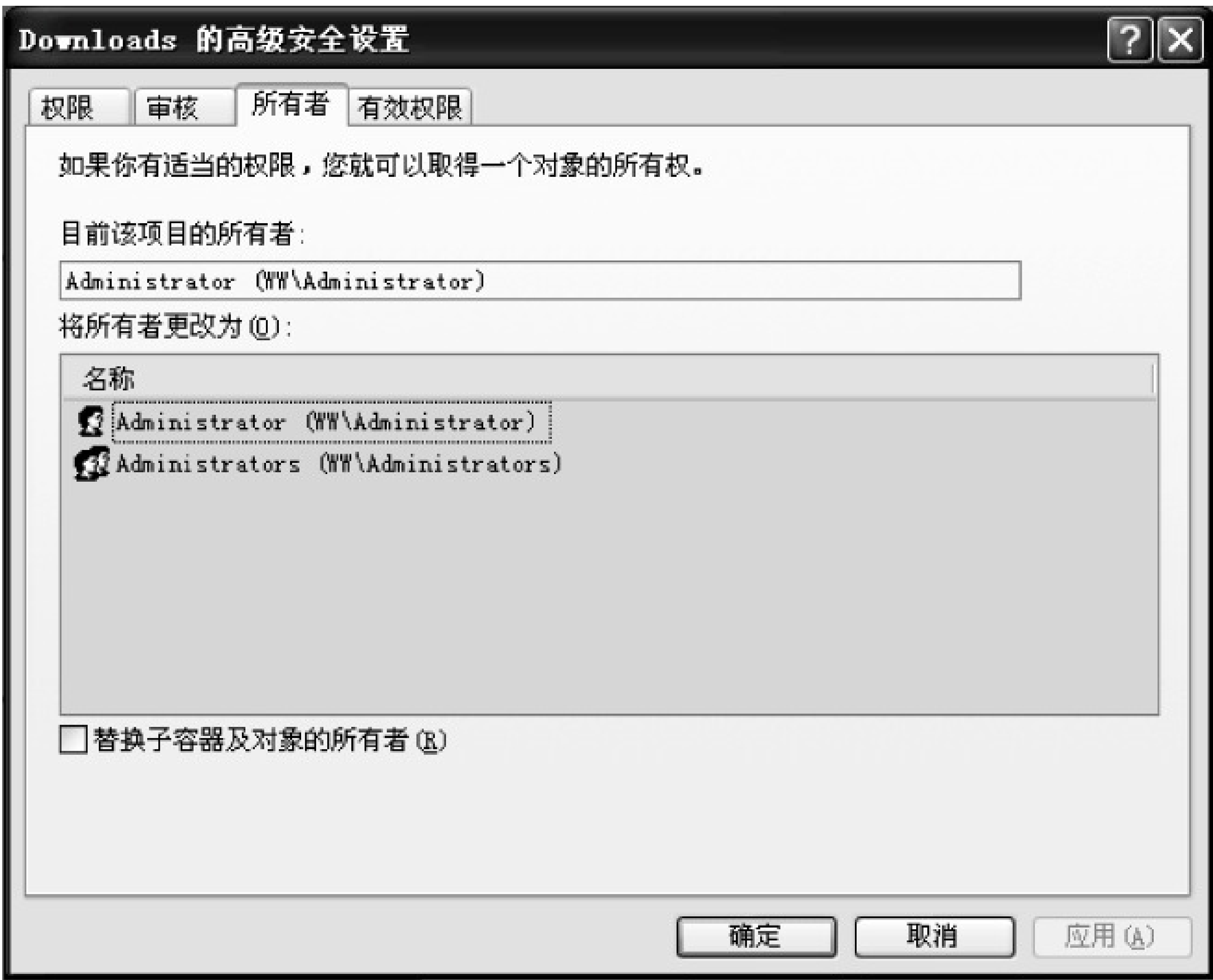


图 6-20　所有者选择

注意:对象取得所有权后,要按照(1)、(2)、(3)描述的步骤设置其他用户的权限后,才能对对象进行操作。该设置包括所有者权限的设置。

4. 共享文件夹

网络的主要作用是资源共享,通过共享文件夹可以实现软件资源的共享。当某个文件夹共享后,网络上的用户在权限许可的情况下,可以访问其中的文件和子文件夹。

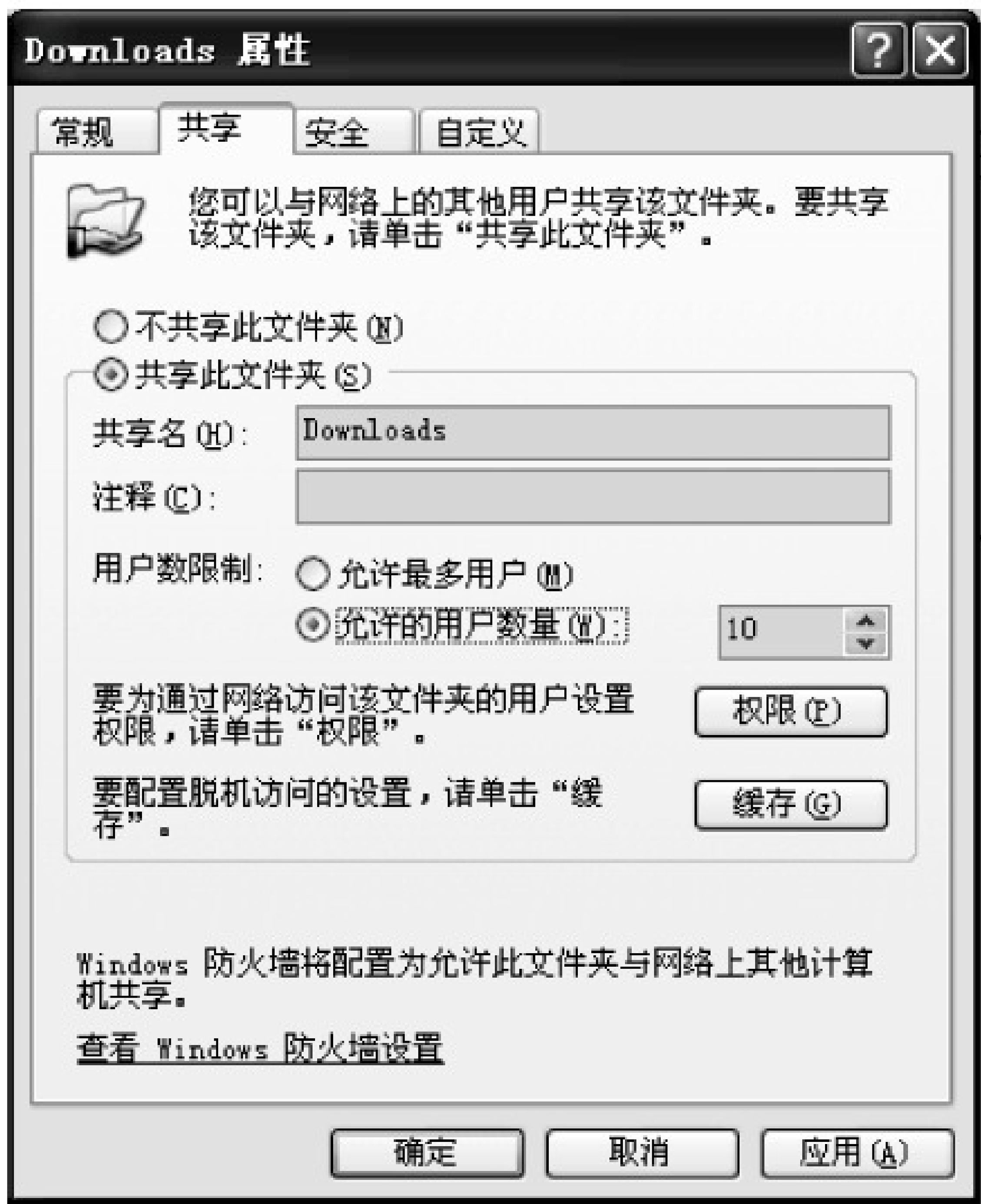


图 6-21　共享设置

(1) 创建共享

Windows Server 2003 成员服务器或独立服务器中创建共享的用户必须有相应的权限,必须是 Administrators 组或 Power Users 组的成员才可以创建共享。在域控制器上创建共享必须是 Administrators 或 Server Operators 组的成员。

设置共享的步骤如下。

右击目标文件夹,选择快捷菜单中的“属性”项,打开“属性”对话框,打开“共享”选项卡;选择“共享此文件夹”单选按钮,输入共享名,用户数限制等,如图 6-21 所示。

(2) 设置共享权限

共享权限是当用户通过网络访问共享文件夹时起作用的,用户在本地访问时不受共享权

限的限制。Windows Server 2003 中，共享权限默认设置是 Everyone 组的成员都有读取的权限。Everyone 组是指共享文件夹所在计算机上的所有本地用户。

① 共享权限的类型

共享权限包括：完全控制、更改、读取三种。

② 共享权限的规则

用户账户的共享权限是他所在用户组和本身所获得共享权限的累积；共享权限也遵守拒绝优先于允许的原则；在网络上访问共享文件夹，如果该共享文件夹在 NTFS 分区上，则用户对共享文件夹的最终权限是其共享权限和 NTFS 权限的交集。

(3) 创建隐藏共享

隐藏共享是在创建共享时，在共享名的后面加上“$”符号，该共享不会在“网上邻居”中出现。操作系统自动创建的默认共享都是隐藏共享，这些共享只能被 Administrators 组的成员访问。可以在“计算机管理”窗口中查看默认共享有哪些，如图 6-22 所示。



图 6-22　隐藏共享文件夹

(4) 访问共享文件夹

① 通过“网上邻居”访问

双击桌面上的“网上邻居”图标，打开“网上邻居”窗口；找到共享文件所在的计算机双击打开；输入用户在该计算机上的账户名和密码，就可以访问共享文件夹。

② 通过网络路径访问

在“运行”对话框或“资源管理器”窗口的地址栏中输入网络路径，可以访问共享文件夹。隐藏共享要在共享名后加“$”。网络路径格式：\\计算机名或计算机 IP 地址\共享文件名。

③ 映射网络驱动器通过资源管理器访问

右击“我的计算机”图标，选择“映射网络驱动器”项；选择驱动器使用的符号，在“文件夹”文本框中输入网络路径、输入访问时使用的用户名和密码。设置完成后，在“我的电脑”中打开相应的网络驱动器访问共享资源。

(5) 管理共享

执行菜单命令“开始”→“程序”→“管理工具”→“计算机管理”，打开“计算机管理”窗口，在窗口左侧展开“共享文件夹”，可以完成共享的管理。

① 共享。可以在其中查看计算机上有哪些文件夹被共享，可以右击选择“停止共享”。

② 会话。可以查看当前哪些用户在使用本计算机上的共享文件，可以关闭会话，停止用户和本地计算机的会话。

③ 打开文件。可以查看哪些用户在使用本地计算机上共享文件夹中的哪个文件，可

以用“将打开的文件关闭”来关闭用户打开的文件。

任务完成：通过前面介绍的内容，配置域控制器，建立组和用户，实现了一个客户机/服务器网络的管理。

任务 6.2　配置 Windows Server 2003 的专用服务器

6.2.1　DNS 服务器的配置

任务描述：创建一个 DNS 服务器，以便完成对建立的各种服务器进行设置，实现域名解析。

任务分解：DNS 服务器主要完成域名的解析，首先需要配置好 DNS 服务器。

1. DNS 服务器基本概念

DNS 是域名系统(Domain Name System)的缩写，指在 Internet 中使用的分配名称和地址的机制。在 Internet 上域名与 IP 地址之间是一一对应的，域名虽然便于人们记忆，但计算机服务器或其他网络设备之间通信只能使用 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

域名解析就是将用户给出的名称变换成网络地址的方法和过程，从概念上讲，域名解析是一个自上而下的过程。当 DNS 客户端给出名称时，接收查询的服务器先从其数据库中寻找，即自己能否解析，若能解析，就将 IP 地址送回客户端；若不能解析，这个任务就转给下一个 DNS 服务器。

(1) DNS 的域名系统空间

DNS 域名系统具有非常分明的层次结构，给域名的查询管理提供了方便。它的结构类似一个树状结构(如图 6-23 所示)，称为域名空间。

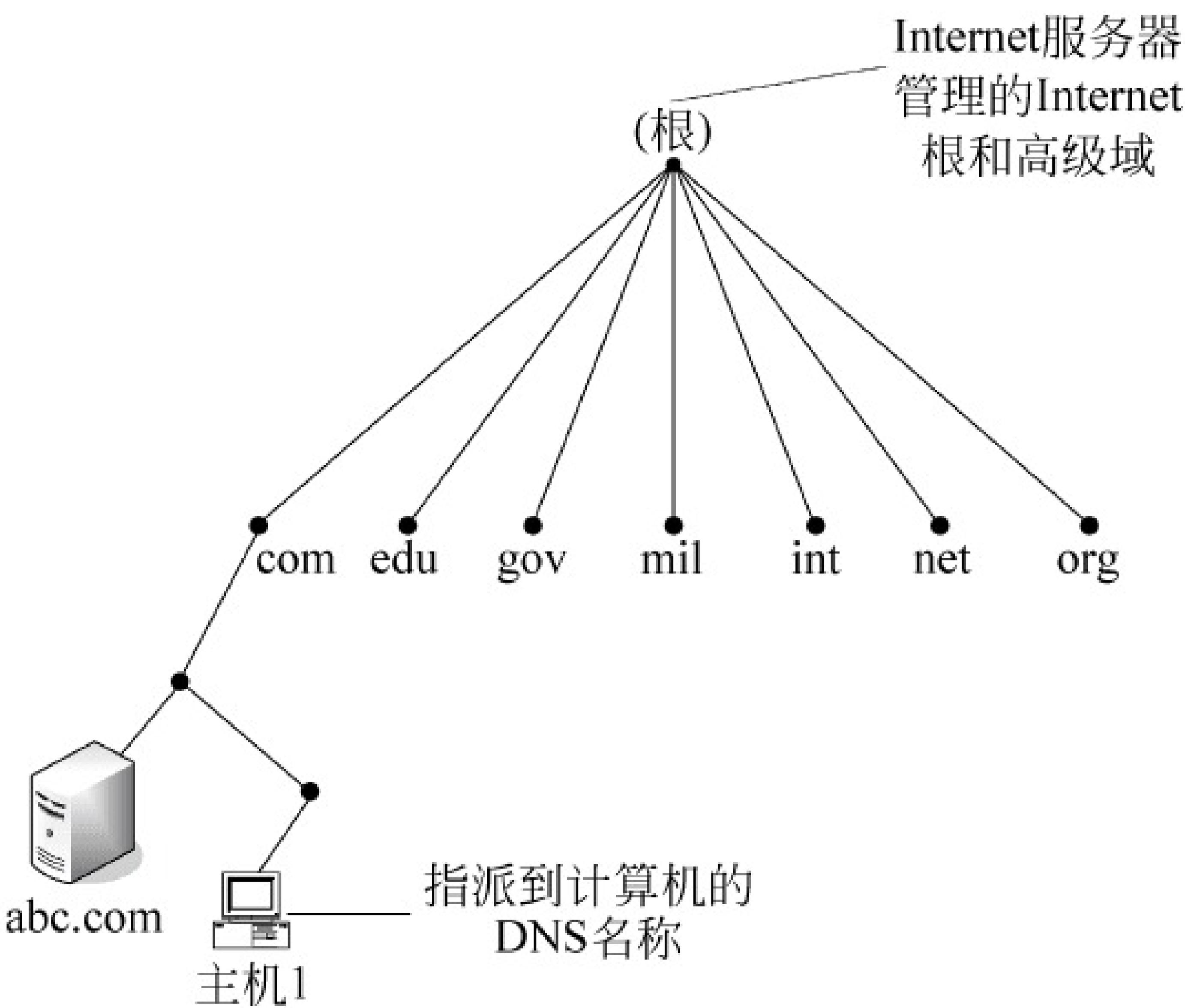


图 6-23　DNS 域名结构图

一棵完整的域树通常由许多大小和位置不同的域组成，来完成分配、改写、查询域名等一系列综合性访问。DNS 系统的核心是 DNS 服务器，在 DNS 服务器上，保存着 DNS 域名空间数据库，并为用户提供各种域名解析服务。在 Internet 上，一个完整的域名结构空间层次由以下几个部分组成。

① 根域。DNS 域名空间的最顶层被称为根域，一般为空，也称空域名。由 Inter NIC 组织负责划分全世界的 IP 地址范围，同时又负责分配 Internet 上的域名结构。

② 顶级域。DNS 域名空间的第二层叫顶级域，是由常用的 com、org、gov、net、edu、mil、int 及国家代码等组成，用于指示国家(地区)或使用者的单位类型。

③ 二级域。DNS 域名空间的第三层是位于顶级域下面的二级域，用来标明顶级域以内的一个特定组织。二级域是为了在 Internet 上使用而由个人或单位注册的长度可变的名称，因此也称注册名。

④ 子域。DNS 域名空间的第四层是二级域下的子域，是由各个组织或单位根据自己的需要自行创建的名称，是从已注册的二级域名中派生出来的。子域下面可派生子域，或者挂接主机。

⑤ 主机。DNS 域名空间的第五层是主机，主机位于 DNS 的最下层，用来标识特定资源(服务或计算机)的名称。

从图 6-23 中可以看出，一个完整的 Internet 域名应当由“主机名＋子域名＋二级域名＋顶级域名”组成。子域与父域之间由“.”隔开，且位于域名空间底层的名称排在前面。

表 6-1 列出了 Internet 中部分顶级域名及其含义。

表 6-1　顶级域的划分

按国家或地区划分		按行业组织划分	
顶级域	含　义	顶级域	含　义
CN	中国	COM	营利性质商业组织
US	美国	NET	网络组织
HK	中国香港	EDU	教育机构
JP	日本	ORG	非营利组织
UK	英国	GOV	政府机构
AU	澳大利亚	MIL	军事机构
TW	中国台湾	INT	国际组织

国际域名由美国商业部授权的 ICANN 负责注册和管理，国内域名则由中国科学院计算机网络中心 CNNIC 负责注册和管理。要想得到合法的域名必须到相关部门注册登记。

(2) DNS 服务器的分类和作用

DNS 服务器是整个 DNS 系统的核心。在 DNS 服务器上，保存着域名空间中的部分区域数据。当一个 DNS 服务器中存放由域名空间内的一个或多个区域的数据时，就称该 DNS 服务器为授权名称服务器。授权名称服务器的分类和作用如下。

① 主要名称服务器。用于存放所在区域中的相关数据。并且主要名称服务器所存

放的是区域文件的正本数据，一个区域内的原始数据库的更新都要在主要名称服务器中进行。也就是说可以在主要名称服务器上创建区域文件，并将其保存在主要名称服务器中，当某个区域文件被修改时，修改后的数据也一同被保存到主要名称服务器中。一个DNS系统中，可以部署多个主要名称服务器，用来在出现故障时的替代。

② 辅助名称服务器。用于从其他服务器中复制数据，并进行保存的服务器。其中的数据不是直接输入的，而是从其他服务器中复制过来的，因此该数据不能修改。当辅助名称服务器启动时，它将与同它建立联系的所有主要名称服务器进行交互，并从中复制数据，它还定期更新原有数据，以保证与主要名称服务器上的数据保持一致。

③ 主控名称服务器。主控名称服务器指提供区域名称数据复制的DNS服务器，它既可以是该区域内的主要名称服务器，也可以是辅助名称服务器。

④ Cache. Only名称服务器。只负责数据查询，并将以往查到的数据保存在高速缓存之中，以便在客户端再次查询该数据时能够快速提供给客户端。它不负责管辖域名称空间内的任何DNS服务器，不创建任何区域，只协助客户端向其他DNS服务器进行查询，将查到的数据备份到高速缓存中，同时响应客户端的查询请求。

⑤ DNS转发器。转发器是一种具有特殊功能的DNS服务器，用来处理内部网络以外的名称查询。若DNS服务器配置为启用转发器，则该DNS服务器会将它在本地无法应答的查询转发给转发器。在规模较大的网络中，转发器也用来将一个网段中的查询转发给另一个网段中的DNS服务器。

DNS服务器被指定为转发器的方法是将其他DSN服务器配置为向此服务器转发其未解析的查询。

(3) DNS查询流程

当DNS客户端需要查询程序中使用的名称时，它会向DNS服务器请求来解析该名称。DNS查询过程按两步进行：名称查询从客户端计算机开始，客户机需要访问网络上的某一主机时，首先向本地DNS服务器查询对方IP地址，并传送至解析程序即DNS客户服务程序进行解析。一般情况下，本地DNS服务器继续向另外一台DNS服务器查询，直到解析出需访问主机的IP地址。不能解析查询时，在客户端显示DNS查询失败。

① DNS查询的种类。DNS的查询有三种：递归查询、迭代查询和反向查询。

递归查询(Recursive Query)。一般客户机和服务器之间属递归查询，即当客户机向DNS服务器发出请求后，则DNS服务器须将正确结果反馈给客户机，若DNS服务器本身不能解析，则会代替客户机向另外的DNS服务器发出查询请求，得到结果后转交给客户机。

迭代查询(Iterative Query)。一般DNS服务器之间属迭代查询，当客户机向DNS服务器发出请求后，该DNS服务器不能解析数据，则它会将下一台DNS服务器的IP地址告诉客户机，这样客户机自己转向下一台DNS服务器查询，以此类推，直到结束，否则最后一台DNS服务器告诉客户机查询失败。

反向查询(Reverse Query)：客户机利用IP地址去解析主机域名的过程。

② DNS域名解析过程。

DNS查询过程按两部分进行：DNS本地解析、查询DNS服务器。

例如：A主机(域名为m1. xyz. com)查询B主机(域名为m2. m3. abc. com)的IP地址。

A 主机首先向本地域名服务器 dns. xyz. com 查询。由于查询不到，就向根域名服务器 dns. com 查询。根据被查询的域名中的“abc. com”，再向授权域名服务器 dns. abc. com 发送查询报文，最后再向授权域名服务器 dns. m3. abc. com 查询。授权服务器返回 m2. m3. abc. com 的 IP 地址送给本地域名服务器 dns. abc. com。本地授权域名服务器 dns. abc. com 将结果返回 com 顶级域名服务器。顶级域名服务器将结果传送给本地域名服务器 dns. xyz. com，它再将查找信息传送给 A 主机。

2. DNS 服务器的安装

选择已经安装了 Windows Server 2003 操作系统的服务器，确认其已安装了 TCP/IP 协议，首先设置服务器 TCP/IP 协议的 DNS 配置，将 DNS 服务器的 IP 地址设为静态。

(1) 执行菜单命令“开始”→“设置”→“网络和拨号连接”，用鼠标右击“本地连接”，选择“属性”项，在协议框中选择“Internet 协议(TCP/IP)”，单击“属性”按钮，打开如图 6-24 所示的对话框。在其中设置 IP 地址、DNS 服务器地址及网关。

(2) 在“控制面板”窗口中单击“添加/删除程序”图标，在弹出的窗口中选择“添加/删除 Windows 组件”项，出现如图 6-25 所示的对话框。

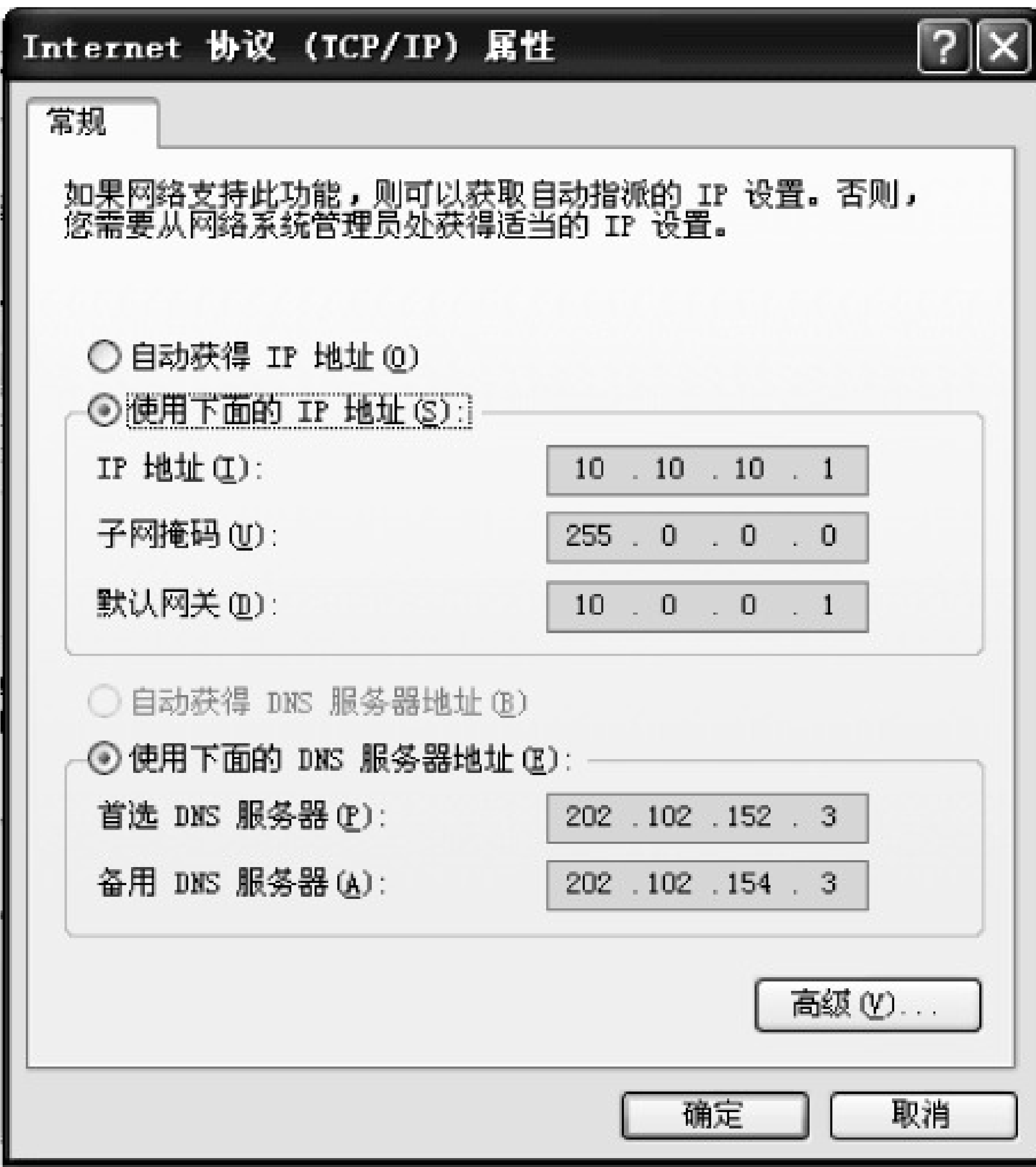


图 6-24　“Internet 协议(TCP/IP)属性”对话框

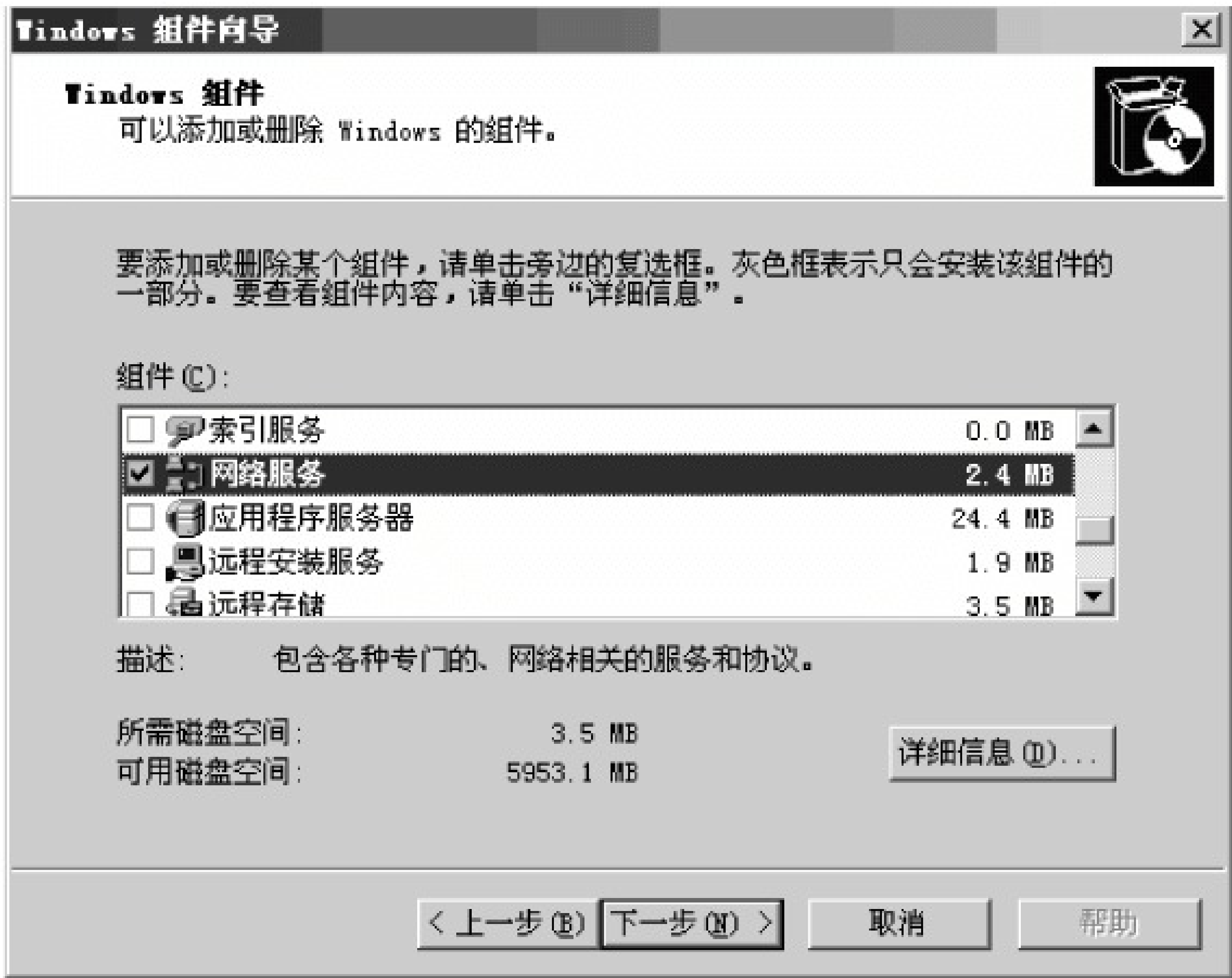


图 6-25 添加 Windows 组件界面

(3) 选择“网络服务”复选框，然后单击“详细信息”按钮，出现如图 6-26 所示的“网络服务”对话框。

(4) 在“网络服务”对话框中，选择“域名系统(DNS)”复选框，单击“确定”按钮，系统开始自动安装相应服务程序。

3. DNS 服务器配置与管理

DNS 服务器以区域为基本的管理单位，里面存储着大量的域名空间里的数据，而且

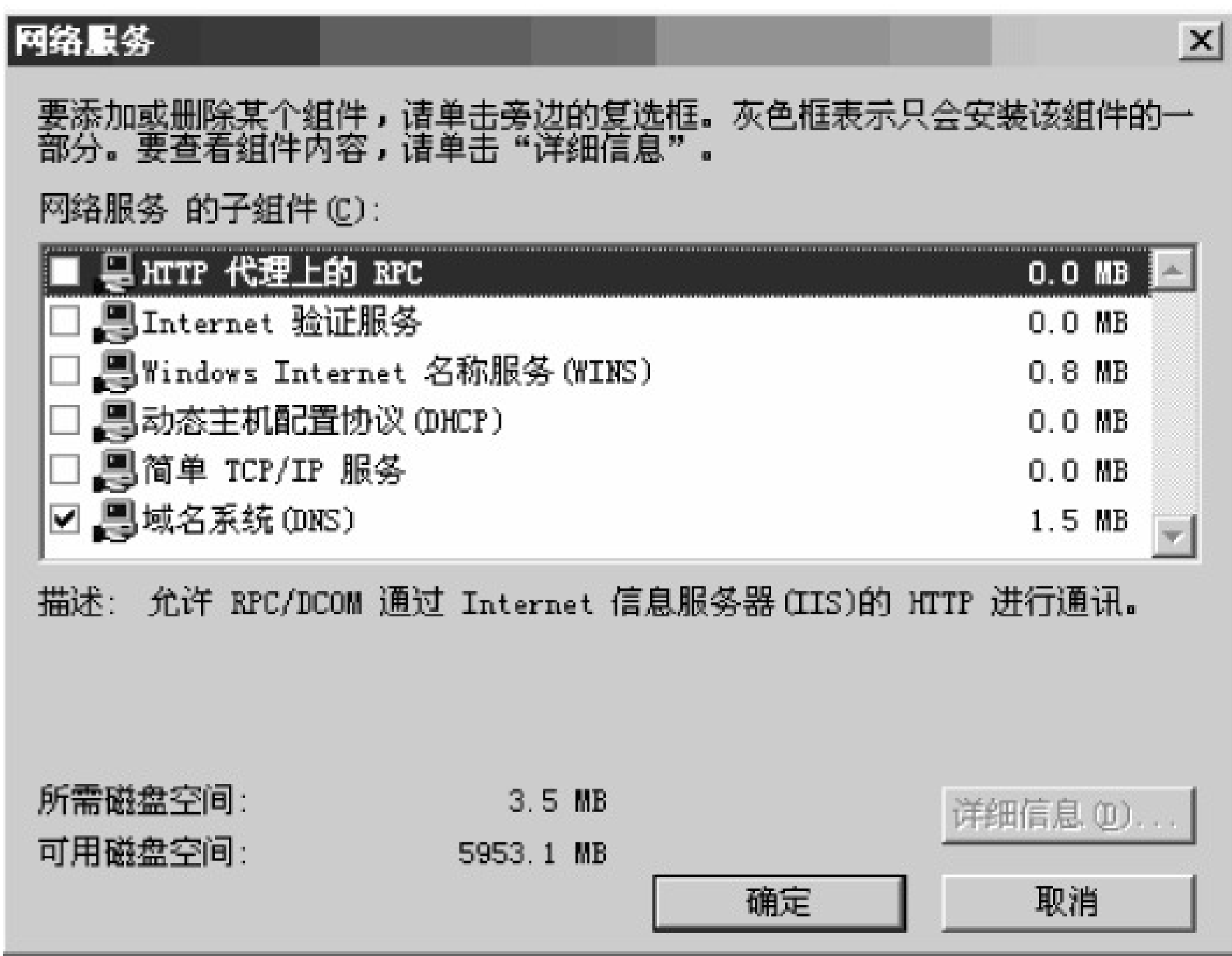


图 6-26 "网络服务"对话框

一台 DNS 服务器可以存储多个区域的数据，所以必须先创立好区域和区域文件，然后再进行设置。DNS 区域分为两类：一类是正向搜索区域，即名称到 IP 地址的数据库，用于提供将名称转换为 IP 地址的服务。另一类是反向搜索区域，即 IP 地址到名称的数据库，用于提供将 IP 地址转换为名称的服务。

（1）添加正向搜索区域

在创建新的区域之前的准备工作：检查一下 DNS 服务器的设置，确认已将"IP 地址"、"主机名"、"域"分配给了 DNS 服务器。检查完 DNS 的设置后，按下列步骤创建新的区域。

① 执行菜单命令"开始"→"程序"→"管理工具"→DNS，打开 DNS 控制台管理器窗口，如图 6-27 所示。

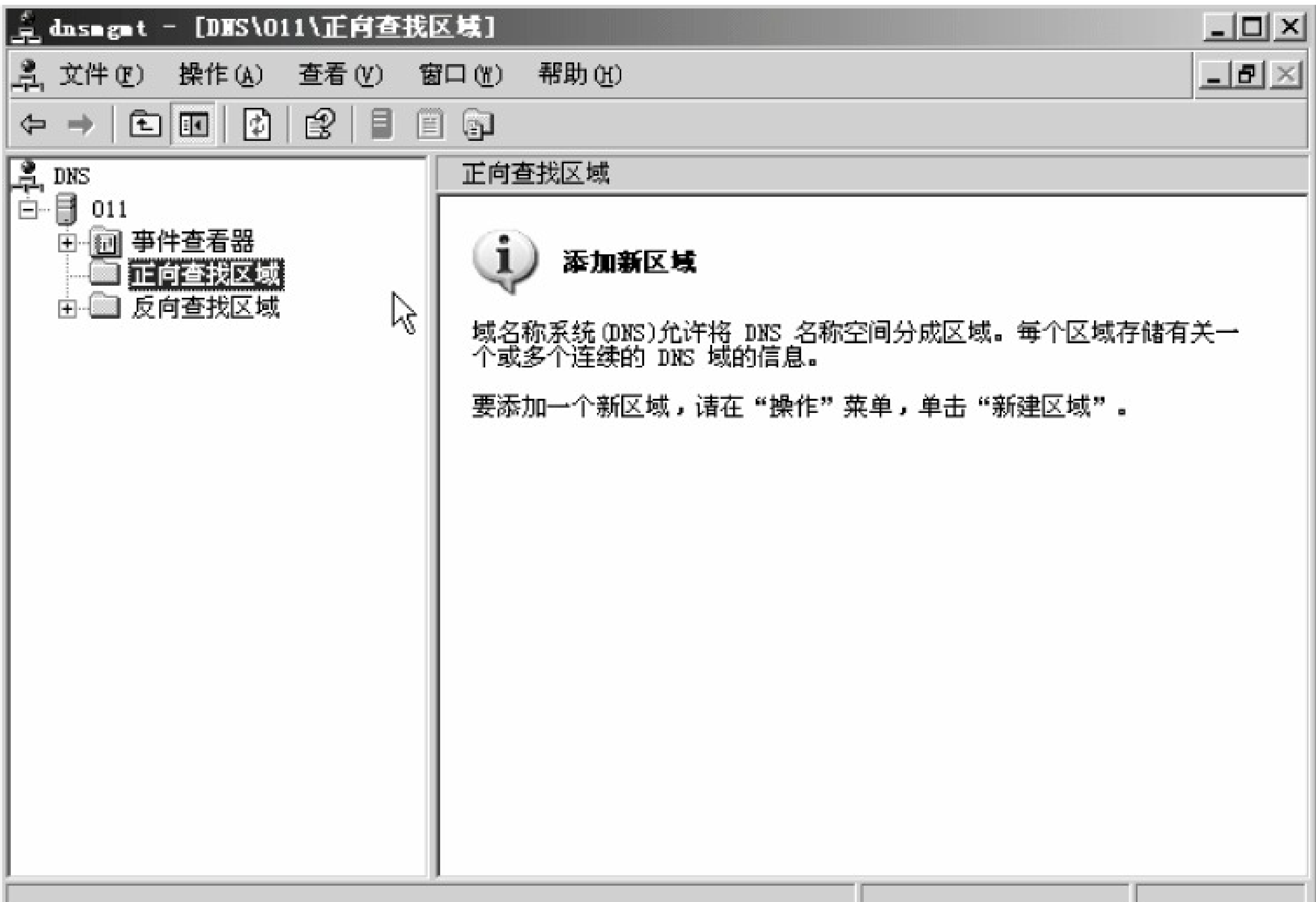


图 6-27 DNS 管理窗口

② 选择要创建区域的 DNS 服务器，右击“正向查找区域”，在快捷菜单中选择“新建区域”，如图 6-28 所示，出现“欢迎使用新建区域向导”对话框时，单击“下一步”按钮。

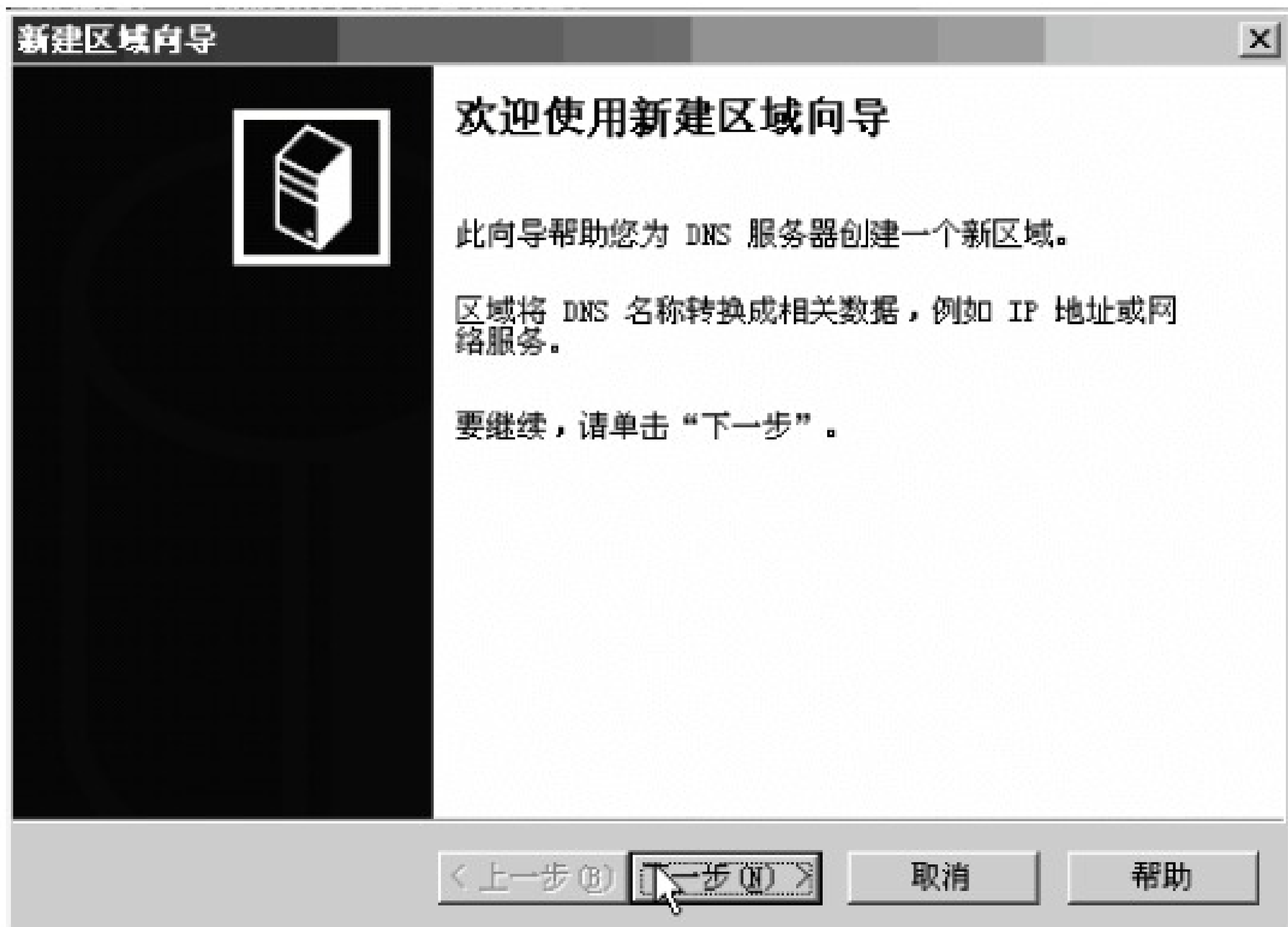


图 6-28　“欢迎使用新建区域向导”对话框

③ 在出现的对话框中选择要建立的区域类型，这里我们一般选择“主要区域”，单击“下一步”按钮。只有 DNS 服务器是域控制器时才可以选择“在 Active Directory 中存储区域”项。

注意：Windows Server 2003 的 DNS 服务器支持以下三种区域类型。

主要区域：存放着该区域内所有的数据记录的正本，当在 DNS 服务器内创建一个主要区域后，该 DNS 服务器就是这个区域的主要名称服务器。

辅助区域：存放着该区域内所有的数据记录的副本，这些副本数据从主要区域中通过区域传送复制过来，这里面的文件只能读取不能修改。创建辅助区域的 DNS 服务器就是这个区域的辅助名称服务器。

存根区域：该区域就是一个区域的副本，只包括标识该区域的权威域名系统服务器所需的那些资源记录。作用是使父区域的 DNS 服务器知道其子区域的 DNS 服务器，保持 DNS 名称解析效率。

④ 在如图 6-29 所示的“区域名称”对话框中，输入新建主区域的区域名，然后单击“下一步”按钮，文本框中会自动显示默认的区域文件名。如果不使用默认的名字，也可以输入不同的名称。



图 6-29　区域名称对话框

⑤ 在出现的对话框中单击“完成”按钮,结束区域添加。

新创建的主区域显示在所属 DNS 服务器的列表中,在完成创建后“DNS 管理器”将为该区域创建一个“起始授权机构记录”,同时也为所属的 DNS 服务器创建一个“名称服务器记录”,并使用所创建的区域文件保存这些资源记录,如图 6-30 所示。



图 6-30 DNS 添加的资源记录

⑥ 添加服务器的主机记录,选中刚才所建区域后,右击鼠标,在快捷菜单中选择“新建主机”项,在弹出的“新建主机”对话框的“名称”文本框中输入新添加的计算机的名字,在“IP 地址”文本框中输入相应的主机 IP 地址。如果要将新添加的主机 IP 地址与反向查询区域相关联,选中“创建相关的指针(PRT)记录”复选框,将自动生成相关反向查询记录,即由地址解析名称,如图 6-31 所示。

⑦ 可重复操作添加多个主机,添加完毕后,单击“确定”按钮关闭对话框,这时候会在“DNS 管理器”中增添相应的记录,如图 6-32 所示。

另外当 DNS 服务器需要更新记录时,它自身具备动态更新功能,当一些主机信息(主机名称或 IP 地址)更新时,更新的数据会自动传送到 DNS 服务器。这要求 DNS 客户端也必须支持动态更新功能。

在 DNS 服务器端必须设置接收客户端动态更新的要求,其设置是以区域为单位的,右击要启用动态更新的区域,选择“属性”项,出现如图 6-33 所示的对话框,选择是否要动态更新。

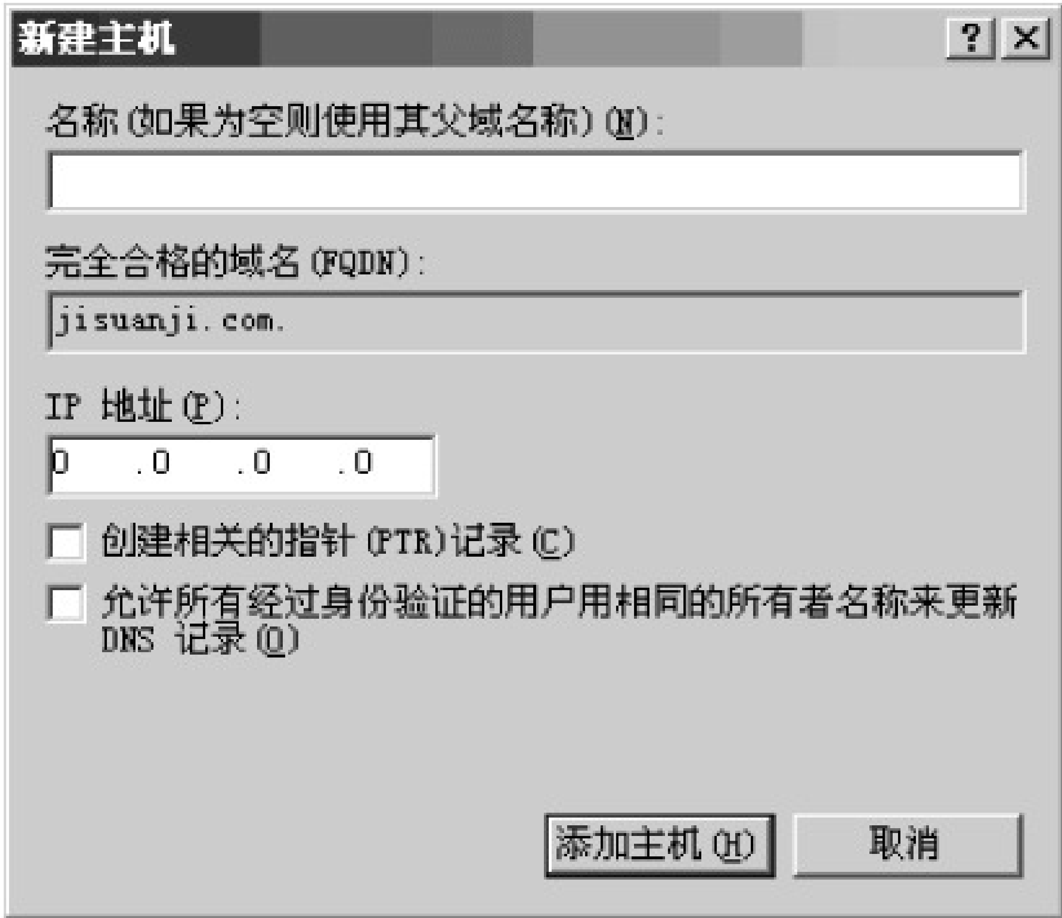


图 6-31 新建主机对话框

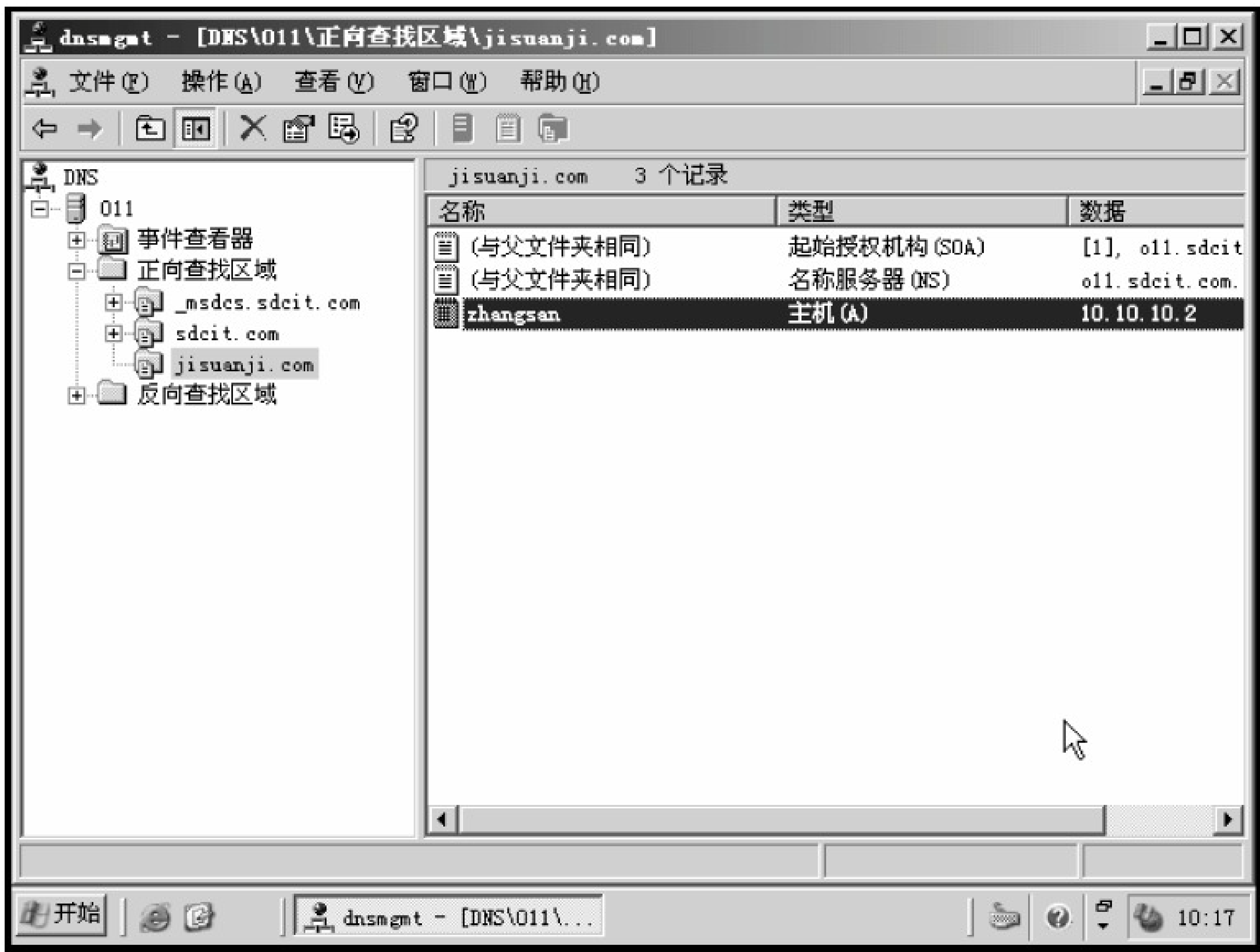


图 6-32　新建主机记录的资源列表

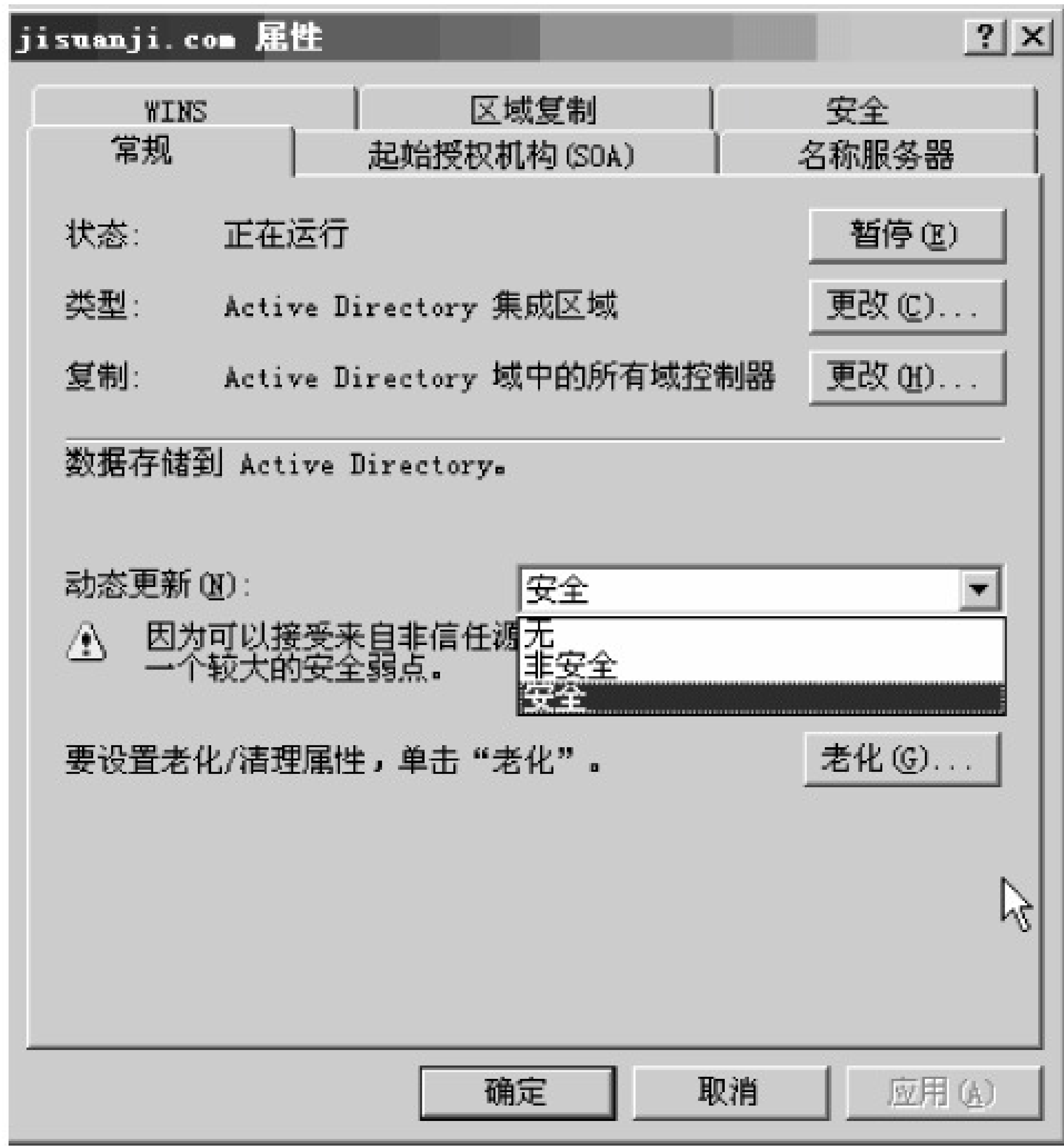


图 6-33　动态更新

(2) 添加反向搜索区域

反向搜索区域可以使 DNS 客户端利用 IP 地址反向查询其主机名称。

添加反向搜索区域的步骤如下。

① 执行菜单命令“开始”→“程序”→“管理工具”→DNS，打开 DNS 管理窗口。

② 在 DNS 管理台中选择要创建区域的 DNS 服务器，右击“反向搜索区域”项，选择快捷菜单中的“新建区域”项，在出现的“欢迎使用新建区域向导”对话框中，单击“下一步”按钮。

③ 在对话框中选择要建立的区域类型，选择“主要区域”，单击“下一步”按钮，只有是域控制器的 DNS 服务器才可以选择“在 Active Directory 中存储区域”。

④ 在弹出的如图 6-34 所示的对话框的“网络 ID”处输入此区域的网络 ID，例如：10.20.30，它会自动在“反向查找区域名称”处设置区“30.20.10.in-addr.arpa”。

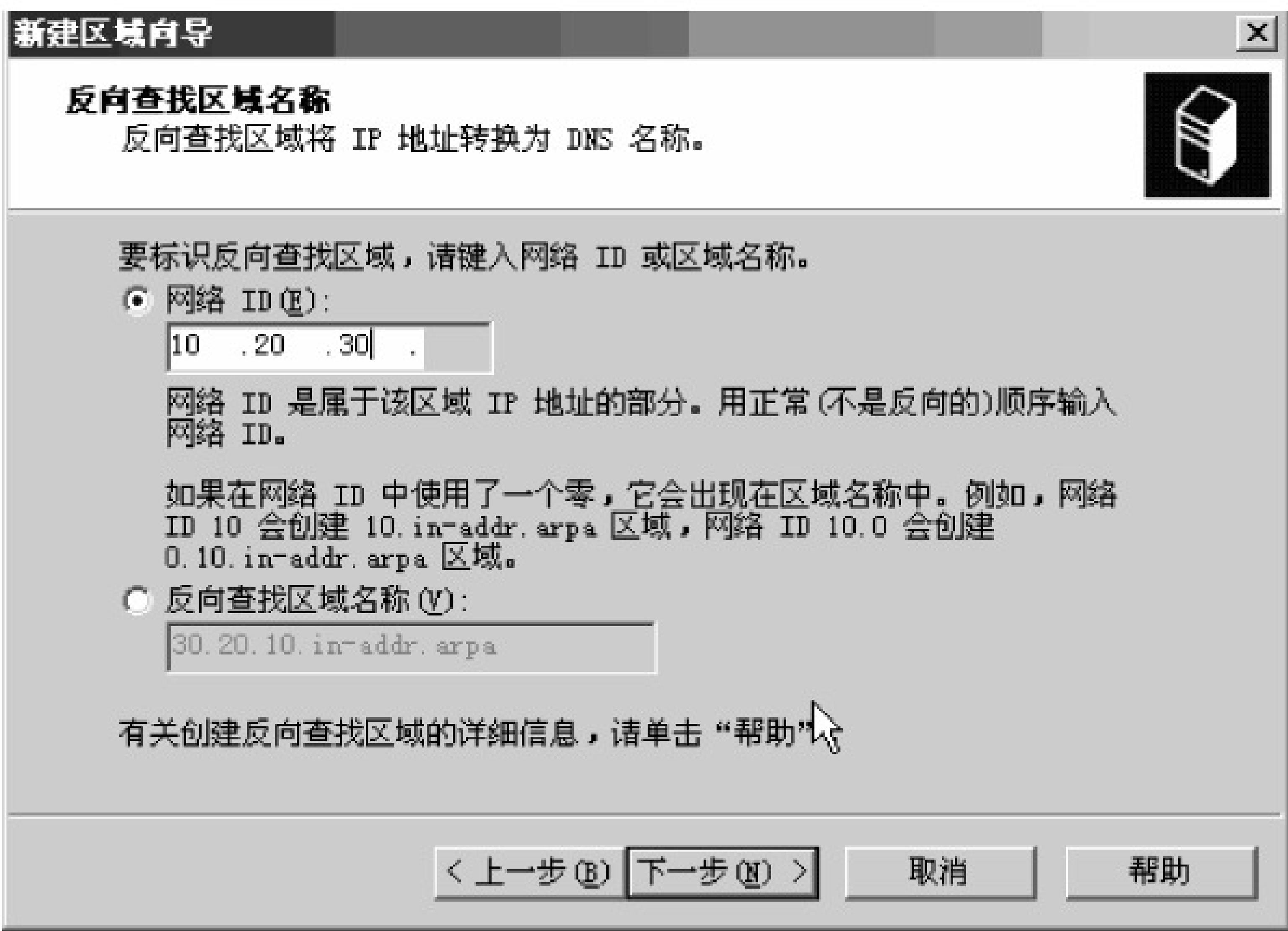


图 6-34　新建反向搜索区域

⑤ 单击“下一步”按钮，文本框中会自动显示默认的区域文件名。如果不使用默认的名字，也可以输入不同的名称，单击“下一步”按钮，完成设置。查看如图 6-35 所示窗口，“10.20.30.x Subnet”就是刚刚创建的反向搜索区域。



图 6-35　反向搜索区域

(3) 添加反向搜索区域的记录

反向搜索区域必须有记录数据以便提供反向查询的服务，下面就是添加反向搜索区域的记录的步骤：

① 选中要添加主机记录的反向主区域 10.20.30.x Subnet，右击鼠标，选择快捷菜单中的“新建指针”。

② 出现如图 6-36 所示的对话框，输入主机 IP 地址和主机的 FQNA 名称，例如：WWW 服务器的 IP 是 10.10.10.1，主机完整名称为 www.abc.com。

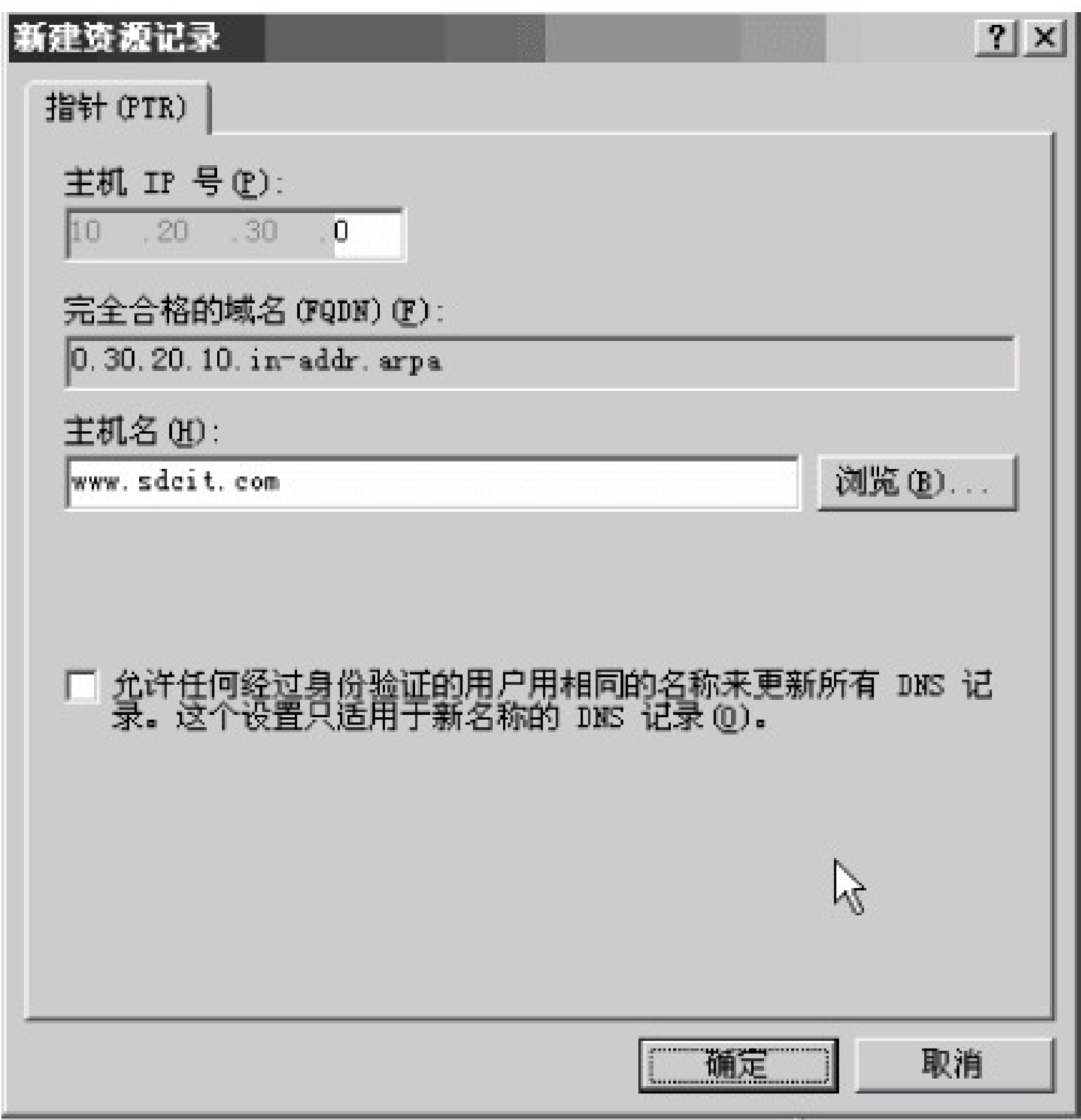


图 6-36　新建指针

可重复以上步骤，添加多个指针记录。添加完毕后，在“DNS 管理器”中会增添相应的记录。

(4) 添加 DNS 资源记录

DNS 除了提供域名到 IP 地址的解析服务之外，还提供了许多其他的服务。这些服务是通过添加适当的资源记录到域中来实现的。除了系统自动创建起始授权机构、名称服务器外，其他的资源记录，用户可根据情况自行向主区域添加。

下面介绍几种记录类型。

① 起始授权机构 SOA(Start Of Authority)。表明该区域的主服务器，是区域数据信息的主要来源。它还指明区域的版本信息，影响区域更新或期满的时间管理主机名称等基本操作。当新区域创建时，该资源记录自动创建。

② 名称服务器 NS(Name Server)。为域标记 DNS 名称服务器，并且出现在所有的 DNS 区域中，是该区域的权威服务器。当新区域创建时，该资源记录自动创建。

③ 主机地址 A(Address)。将主机的 DNS 域名映射到计算机使用的 IP 地址，是常用的资源记录类型，可以手动创建主机记录。当 IP 地址配置更改时，运行的计算机可以动态注册和更新它们在 DNS 中的主机记录。

④ 指针 PTR(Point)。在反向搜索区域中创建的一个映射，用于把计算机的 IP 地址映射到 DNS 反向搜索区域的域名，它仅用于支持反向搜索。可以静态手动创建指针记录，也可以在创建主机记录时创建相关的指针记录；当 IP 配置更改时，运行的计算机可以动态注册和更新它们在 DNS 中的指针记录。

⑤ 邮件交换器资源记录 MX(Mail eXchange)。为 DNS 域名指定邮件交换服务器。邮件交换器资源记录由电子邮件系统使用，用以根据在邮件目标地址中的 DNS 域名来定位邮件服务器。

⑥ 别名 CNAME(Canonical Name)。主机的另一个名字，将 DNS 域名的别名映射到另一个主要的名称。允许用多个名称指向一个主机。

(5) 设置转发器

域内的 DNS 服务器只负责本网络内的域名解析，要想解析其他域内的域名，只能通过设置“转发器”，通过上一级 DNS 服务器完成。

设置步骤：首先在“DNS 管理器”窗口中选择 DNS 服务器，右击鼠标，选择“属性”

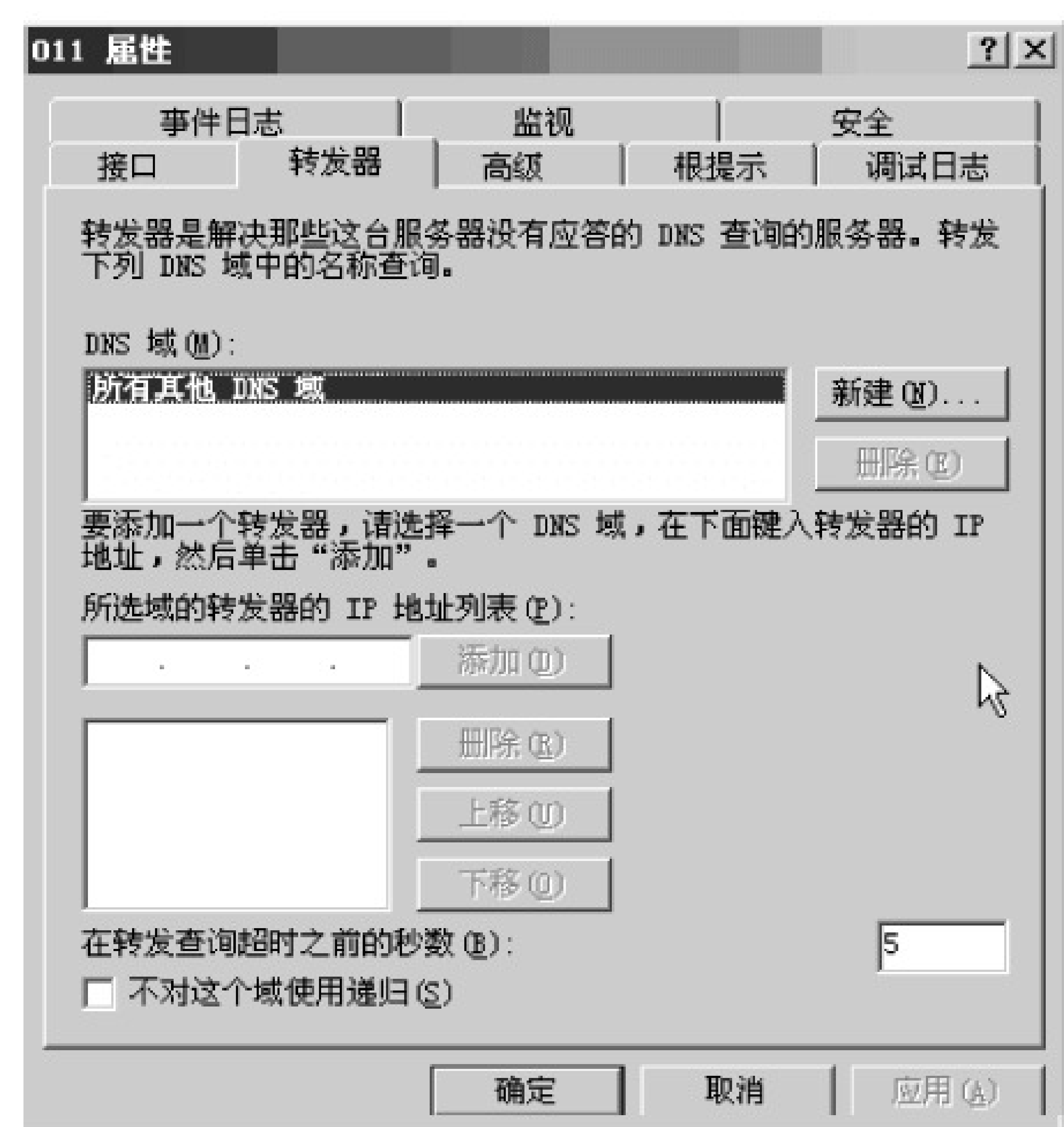


图 6-37　转发器设置

项，打开“转发器”选项卡，在弹出的如图 6-37 所示的对话框中新建或选择一个 DNS 域，为该域设置转发器的 IP 地址列表。

（6）建立辅助区域

辅助区域可将上级区域的所有内容复制过来，以保持同步。上级区域可以是主要区域，也可以是辅助区域。可在网络上安装多台 DNS 服务器，其中一台建立主要区域，其他的 DNS 服务器建立辅助区域。

辅助区域需要从上级 DNS 服务器复制区域信息，要完成这一任务，在建立辅助区域的时候，需要在上级服务器上为其授权。

例如以 sdcit.com 为例，在 DNS 服务器 1（计算机名 xxgc1、IP 地址 10.10.4.3）上建立 sdcit.com 主要区域，在 DNS 服务器 2（计算机名 xxgc2、IP 地址 10.10.4.10）上建立 sdcit.com 的辅助区域的方法。

① 在 DNS 服务器 xxgc1 上建立 sdcit.com 主要区域。

② 右击 sdcit.com 区域，从弹出的快捷菜单中选择“属性”项，打开“区域复制”选项卡。如图 6-38 所示。

③ 在“区域复制”选项卡中，选择“允许区域复制”复选框，选择有哪些服务器可以复制 sdcit.com 区域信息到所有服务器。

网络里任何一台服务器都可以复制 sdcit.com 区域的信息。

只有在“名称服务器”选项卡中列出的服务器。“名称服务器”选项卡列出当前活动目录里所有的 DNS 服务器，也可以手动添加其他的 DNS 服务器，如图 6-39 所示。

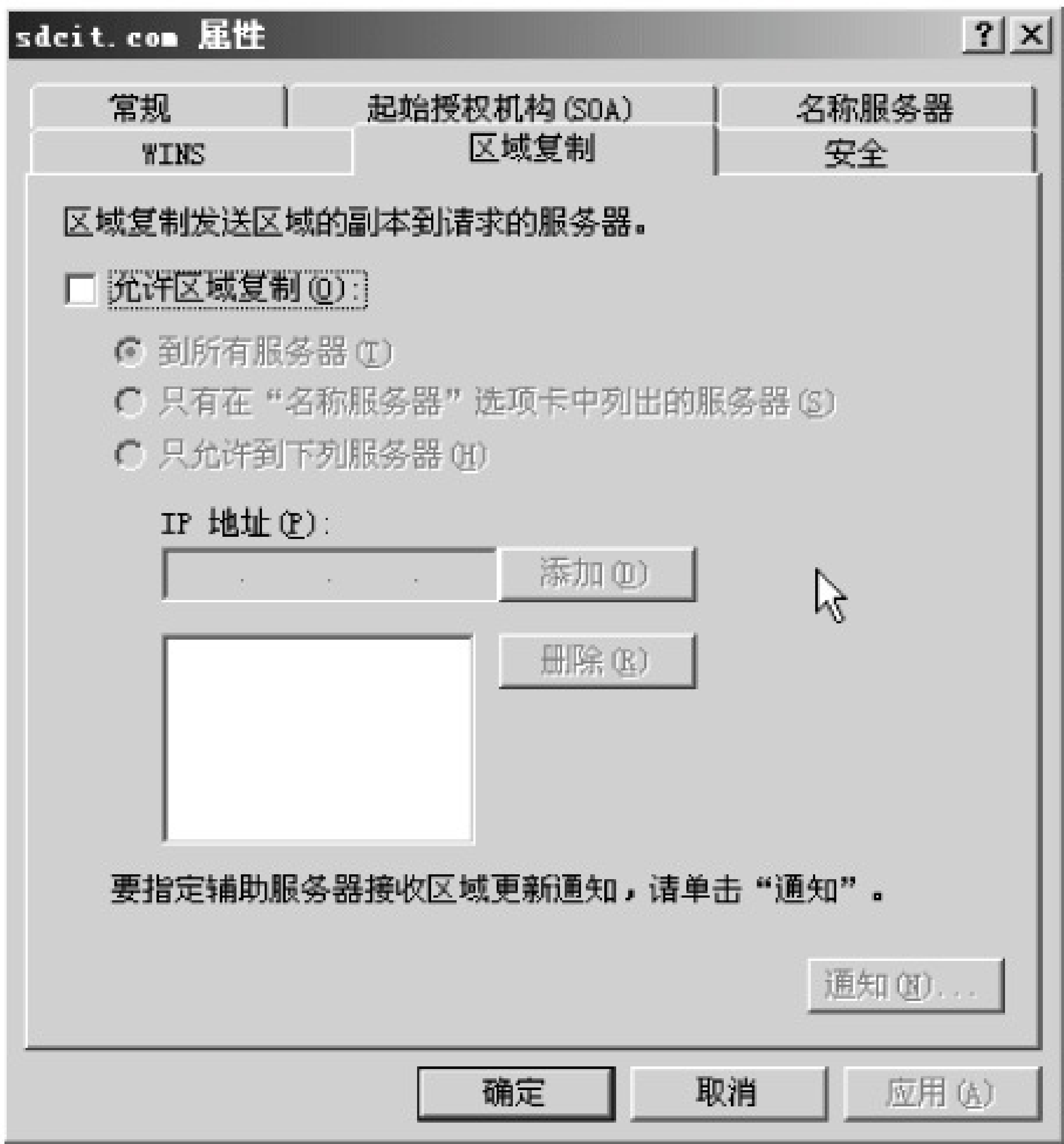


图 6-38　“区域复制”选项卡

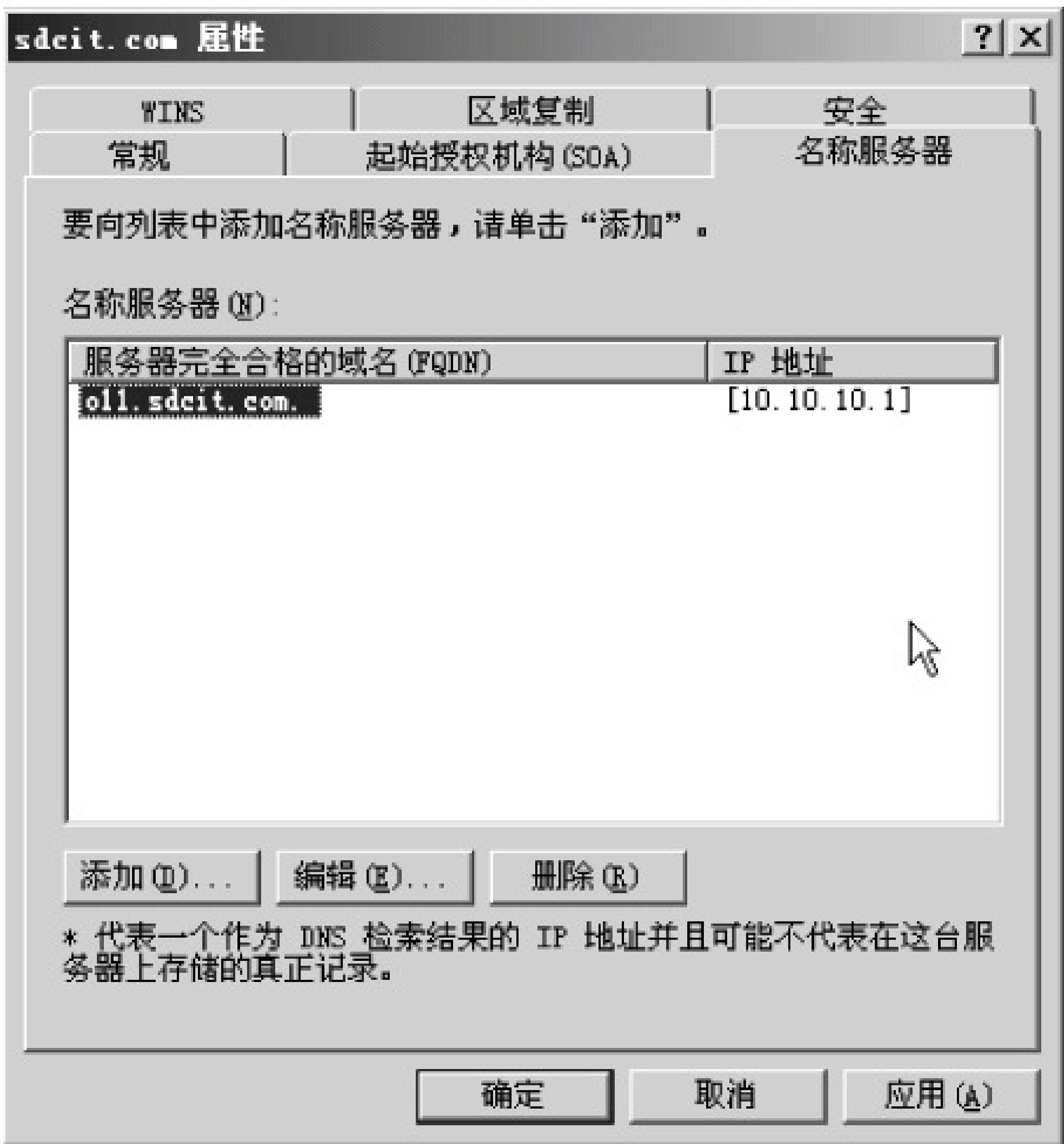


图 6-39　“名称服务器”选项卡

只允许到下列服务器。可以手动指定某几台 DNS 服务器允许复制 sdcit.com 区域信息。如果希望 DNS 服务器 xxgc2 能够从 DNS 服务器 xxgc1 上复制 sdcit.com 区域信息,必须启用允许区域复制。

④ 在 DNS 服务器 xxgc2 上,打开 DNS 管理控制台,右击“正向查找区域”选项,从快捷菜单中选择“新建区域”选项,在“新建区域向导”对话框中,选择区域类型为“辅助区域”,单击“下一步”按钮。

⑤ 输入区域名称 sdcit.com,如图 6-40 所示,单击“下一步”按钮。

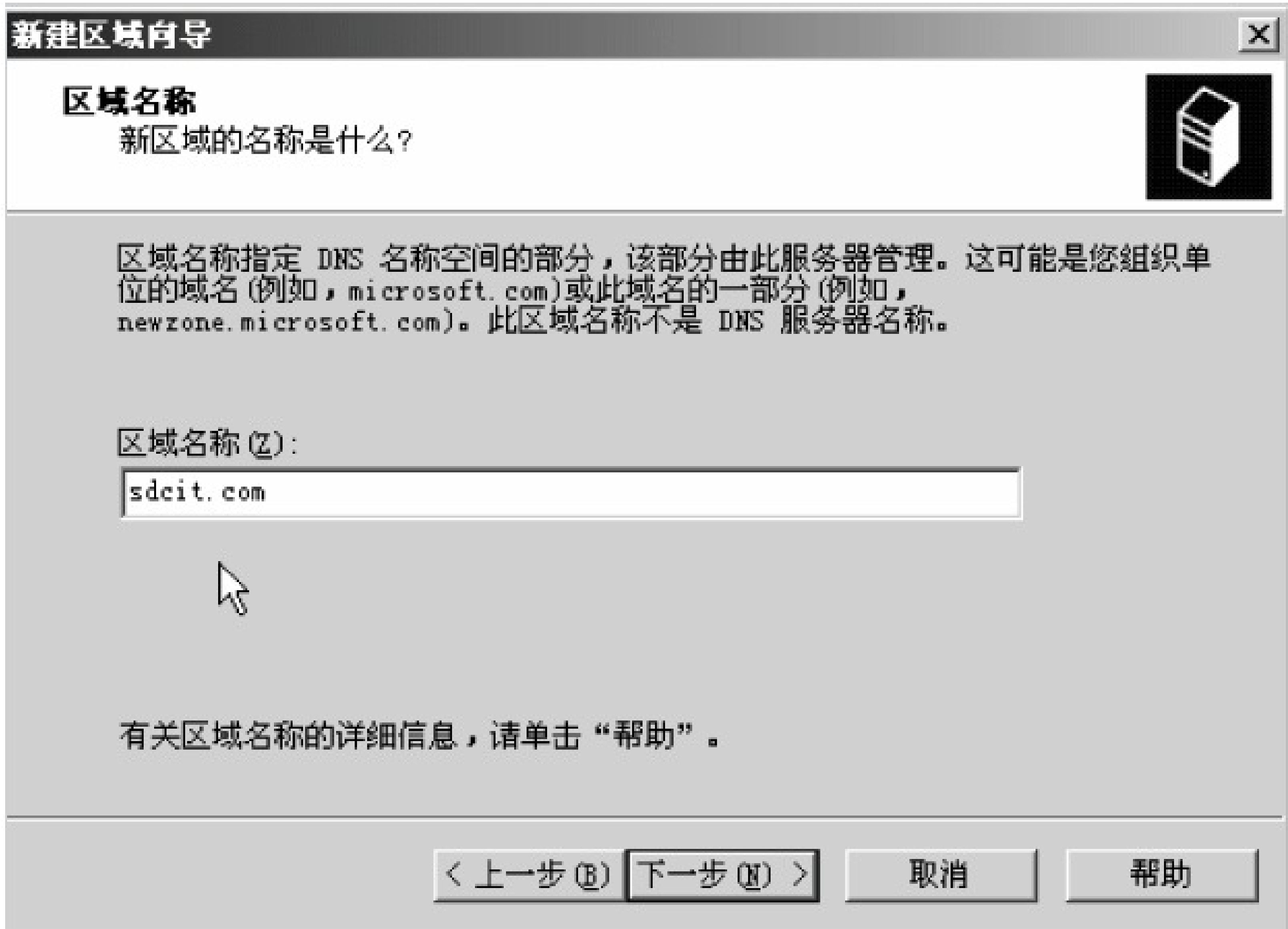


图 6-40 输入辅助区域的名称

⑥ 输入 DNS 服务器 xxgc1 的 IP 地址 10.10.4.3,如图 6-41 所示。

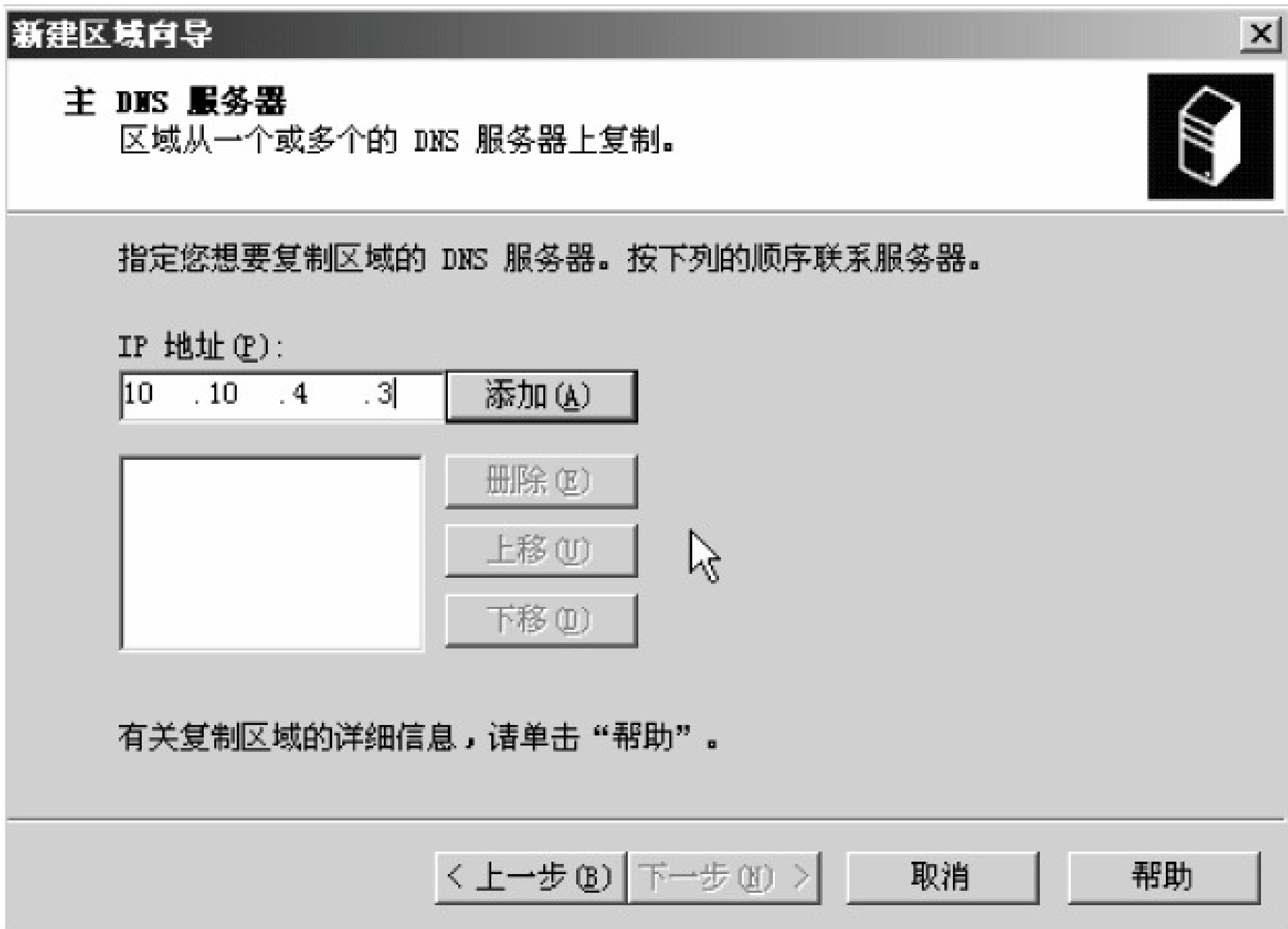


图 6-41 输入上级区域服务器的 IP 地址

⑦ 单击“完成”按钮,结束设置。

注意:辅助区域不能建立、修改和删除区域内的资源记录,会自动从主要区域复制所有信息。

6.2.2 Web 服务器的配置

任务描述：在一台安装了 Windows Server 2003 系统的服务器上，存放着某公司的一个宣传网页，利用 IIS 服务将这个网站发布出去。

任务分解：提供网页访问服务，需要在服务器上安装 Web 服务器。

1. Web 的概念

WWW 是 World Wide Web 的简写，又称为 Web 或万维网。最初由欧洲粒子物理实验室于 1989 年开发。Web 服务给人们提供了查询、共享信息和进行多媒体交互的手段。Web 是建立在客户机/服务器模式上的，以 HTML 语言和 HTTP 协议为基础的，是目前应用最广泛的网络服务，世界上大多数站点都采用 Web 服务器发布信息。

Web 服务器利用超文本链接页面，这些网页可以放在同一台服务器上，也可在不同的服务器上，访问时用 URL（统一资源定位符）确定位置，Web 客户机通过相应的软件如 IE 浏览器向服务器发出请求。

2. 安装 IIS

IIS（Internet Information Server）是集成 Web 服务、FTP 服务、SMTP 服务和 NNTP（Network News Transfer Protocol）服务于一体的 Internet 信息服务系统。Web 服务用来架设 Web 站点，并支持 Web 内容的保存与更新的服务；FTP 服务器用于架设 FTP 站点，提供上传与下载文件的服务；SMTP 和 NNTP 分别用于邮件发送和网络新闻服务。

在配置 Web 服务、FTP 服务、SMTP 服务和 NNTP 服务之前，首先要安装 IIS。

（1）以 Administrator 的身份登录服务器，执行菜单命令"开始"→"控制面板"，单击"添加或删除程序"图标，单击"添加/删除 Windows 组件"按钮。在出现的如图 6-42 所示的"Windows 组件向导"对话框中，选择"应用程序服务器"复选框，单击"详细信息"按钮。



图 6-42 "Windows 组件向导"对话框

（2）出现如图 6-43 所示的"应用程序服务器"对话框，选择"Internet 信息服务（IIS）"复选框，单击"详细信息"按钮。

（3）出现如图 6-44 所示的“Internet 信息服务（IIS）”对话框，安装 WWW 服务，选择“万维网服务”复选框，单击“确定”按钮，开始安装，单击“下一步”按钮，按提示操作，单击“完成”按钮，结束安装。

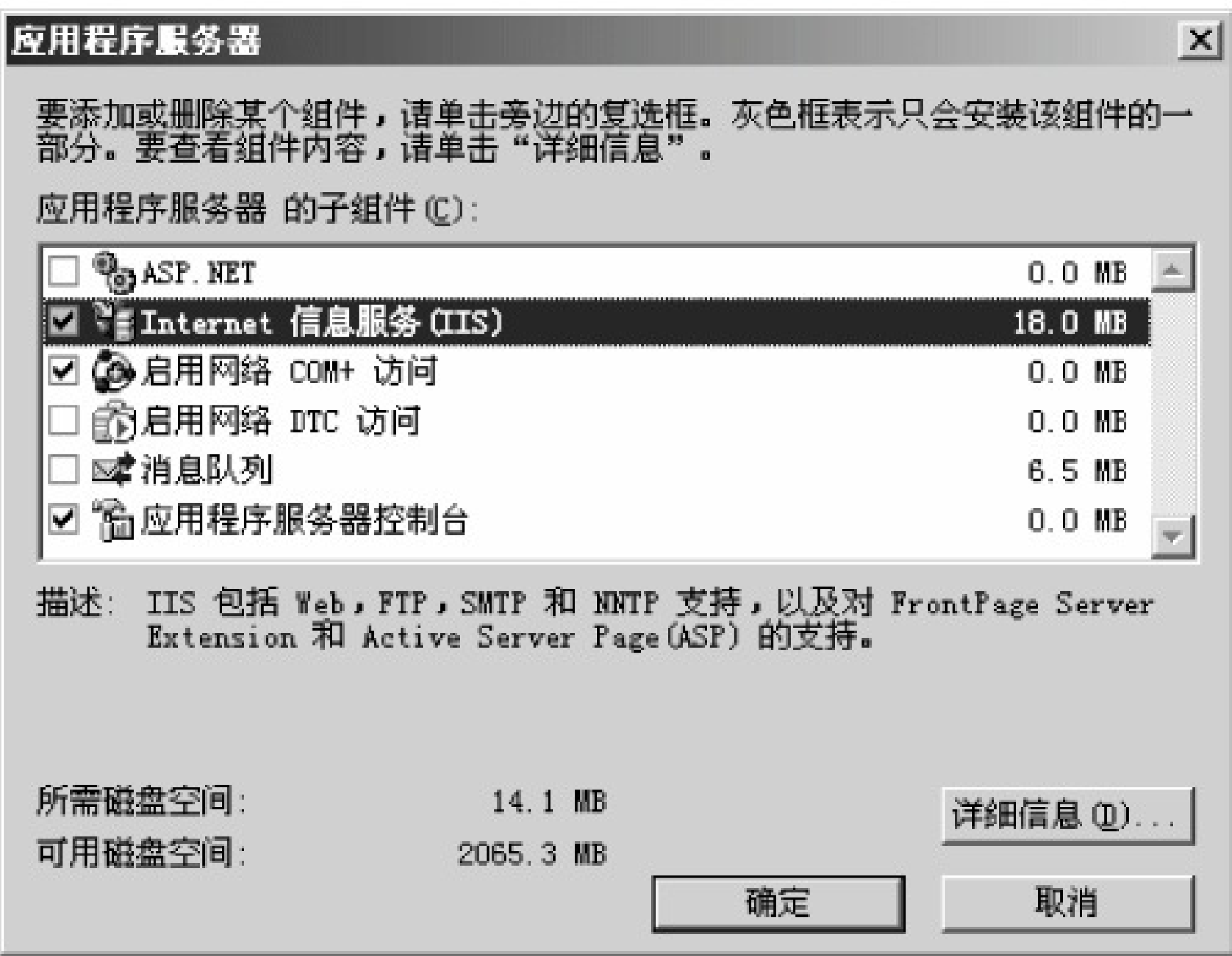


图 6-43 “应用程序服务器”对话框

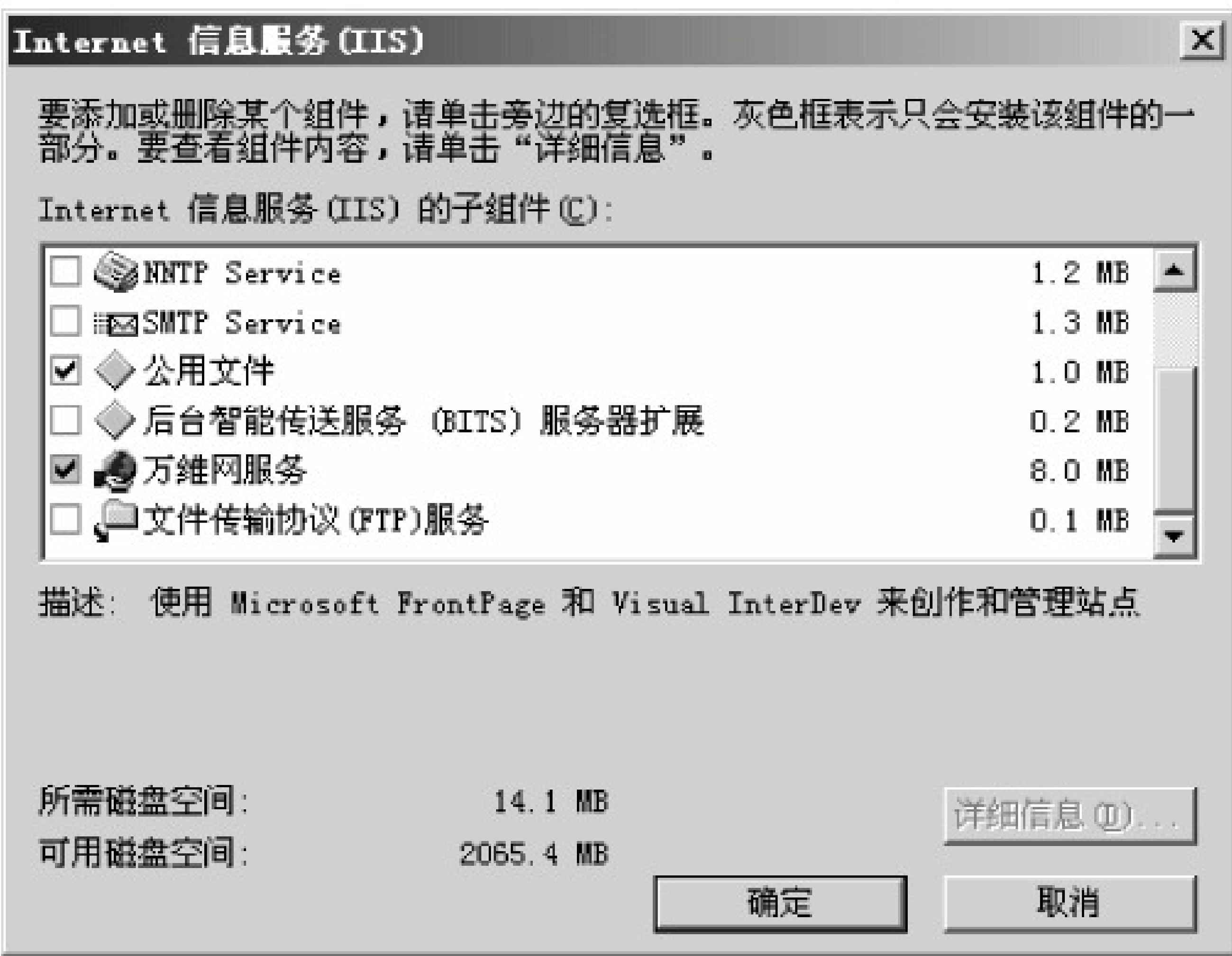


图 6-44 “Internet 信息服务（IIS）”对话框

3. 配置 Web 服务器

（1）新建 Web 站点

在“Internet 信息服务（IIS）管理器”窗口中，可以创建和管理多个 Web 站点，新建 Web 站点的步骤如下：

① 以 Administrator 的身份从服务器登录，执行菜单命令“开始”→“程序”→“管理工具”→“Internet 信息服务（IIS）管理器”，打开“Internet 信息服务（IIS）管理器” 窗口，如图 6-45 所示。



图 6-45 “Internet 信息服务（IIS）管理器”窗口

② 在“Internet 信息服务（IIS）管理器”窗口中，展开要设置的服务器，右击“默认网站”选项，选择快捷菜单中的“属性”项，打开“默认网站属性”对话框，在“网站”选项卡中，设置网站使用的 IP 地址和端口号，以及连接超时时间和是否启用日志。

③ 打开“主目录”选项卡，在“本地路径”输入自己网页所在的目录，单击“确定”按钮。

④ 打开IE浏览器，在地址栏输入IP地址后按Enter键，则能够调出网页的首页。说明设置成功。

注意：建立站点前要确定好静态IP地址和DNS域名，并建立相应的DNS解析；建立网站的主目录，在主目录内设置主页文件名default.htm、default.asp、index.htm或default.aspx。

（2）创建虚拟目录

右击“默认网站”选项，从弹出的快捷菜单中选择“新建”→“虚拟目录”项，打开“性能目录创建向导”对话框，单击“下一步”按钮。

打开“虚拟目录别名”对话框，在“别名”文本框中输入设定的别名如“mchy”，单击“下一步”按钮。

打开“Web网站内容目录”对话框，在“目录”文本框中输入包含网站内容的目录的路径，单击“下一步”按钮。

打开“虚拟目录访问权限”对话框，设置访问权限，单击“下一步”按钮。虚拟目录访问权限包括读取、允许脚本、执行、写入、浏览等。

打开“已完成虚拟目录创建向导”对话框，单击“完成”按钮可设置成功。

（3）创建多个站点

在一个IIS服务器上创建多个Web站点可以使用三种方法：使用不同的IP地址创建多个网站，使用同一个IP地址、不同端口号创建多个网站，使用不同的主机头名创建多个不同的网站。创建的步骤如下。

① 在“Internet信息服务(IIS)管理器”窗口中，选择需添加Web站点的计算机名展开。

② 右击“默认网站”项，在弹出的快捷菜单中选择“新建”→“网站”命令。

③ 打开“网站创建向导”窗口，单击“下一步”按钮，在弹出的对话框中输入站点说明。

④ 单击“下一步”按钮，在弹出的对话框中指定Web站点的IP地址和TCP端口号等信息(其中还有主机头的信息，用于当多个站点对应一个主机地址之时区分站点之用)。

⑤ 单击“下一步”按钮，在弹出的对话框中指定Web站点信息所在的文件夹，即用户通过浏览器所看到的Web站点信息所存放的位置，在这里单击“浏览”按钮为站点选择一个主目录，并选中“允许匿名访问网站”复选框，如图6-46所示。



图6-46　主目录路径设置

⑥ 单击“下一步”按钮，在弹出的对话框中设定对于主目录的访问权限。对于绝大多数客户端来说，只需设定浏览、读取的权限就可以了，如图 6-47 所示。



图 6-47　网站访问权限设置

⑦ 单击“下一步”按钮，按提示完成 Web 站点的创建。

注意：使用不同的主机头创建多个不同的网站，首先需要在 DNS 服务器中将所有主机名做好映射。在建立时，使用默认网站。在“属性”对话框的“IP 地址”栏中选择了 IP 地址后，单击右侧的“高级”按钮。在弹出的对话框中，在“此网站的多个标识”文本框双击已有的 IP 地址，打开“添加/编辑网站标识”对话框，在“主机头值”文本框中输入主机头名，单击“确定”按钮。

(4) 管理 Web 站点

执行菜单命令“开始”→“程序”→“管理工具”→“Internet 信息服务(ISS)管理器”，打开“Internet 信息服务(IIS)管理器”窗口，在所管理的网站上右击，选择“属性”菜单项，进入该站点的“属性”对话框，如图 6-48 所示。

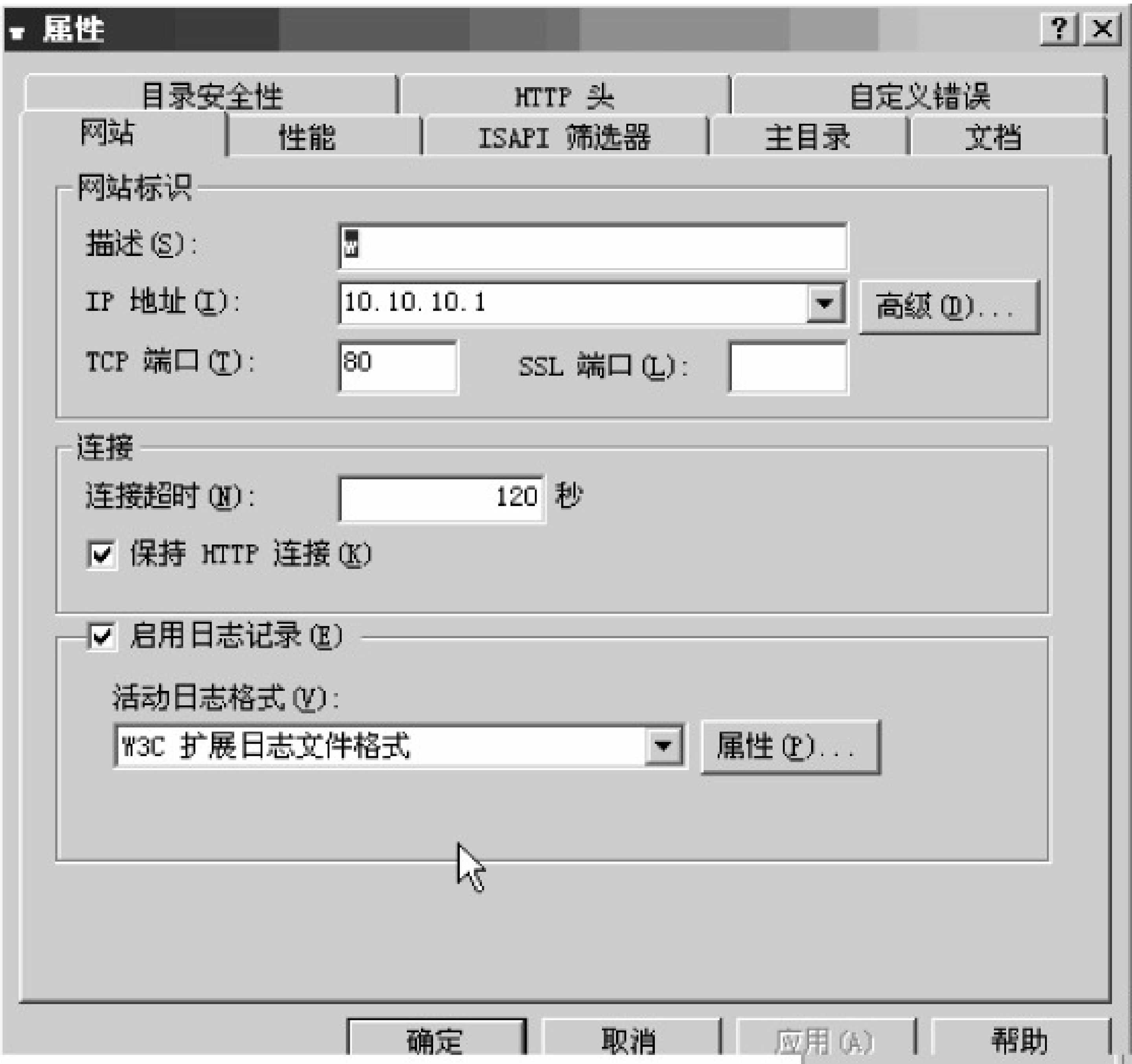


图 6-48　Web 属性设置

①“网站”属性

可以设置 Web 站点的标识、连接设置和日志等,如图 6-48 所示。

描述:文本框中输入任何文字作为该 Web 服务器的名称,这一名称将显示在控制台的目录树中。

IP 地址:设置该站点使用的 IP 地址。一个站点可以设置多个 IP 地址,如果选择使用多个 IP 地址可以通过“高级”设置。

TCP 端口:为网站运行时数据通过计算机的 TCP 端口号码,默认情况下为 80,也可以设置其他的号码。

SSL 端口:安全套接字层端口号。

连接超时:设置服务器断开与未活动用户的时间。防止用户长期占据连接而无任何操作。

保持 HTTP 连接:允许客户与服务器保持开放连接,不必让用户新的请求再次打开一个连接。

启用日志记录:记录用户操作的细节。在活动日志格式下拉框中选择日志格式,主要有 Microsoft IIS 日志格式(一种固定的 ASCII 格式)、NCSA 公用日志文件格式(国家超级计算机应用中心的公用格式)、W3C 扩展日志文件格式(一种可以自行定制的格式)、ODBC 日志(记录到数据库)。

②“主目录”属性

可以设置:此计算机上的目录或者另一计算机上的共享位置,Web 站点的有关默认目录,Web 站点的默认主目录是“c:\kinetpub\wwwroot”,以及重新定位到 URL、执行权限、应用程序池等选项。

此资源的内容来自:

选择“此计算机上的目录”项,可以在“本地路径”文本框后,单击“浏览”按钮设置默认的主目录。

选择“另一台计算机上的共享”,在另外的计算机上共享的资源。

选择“重定向到 URL”,在网络中共享的资源。

在下列访问权限中,有 6 个复选框可以进行设置。

“脚本资源访问”:该选项仅在选中了“读取”或“写入”时才生效。

读取:选中了该复选框时,允许用户读取或下载存储在该站点上的主目录,如果没有选中该选项,访问者将得到错误信息。

写入:选中该复选框时,用户可以在相应被允许修改的浏览器中对该站点进行写入操作,可以上传文件。

目录浏览:选中该复选框时,当用户在浏览器的地址栏中没有指定访问的文件,而该站点又没有默认文档时,将发送给用户一个超文本的虚拟目录列表,使用户访问“日志访问”记录。

日志访问:选中该复选框时,在站点的日志文件中记录着用户对该目录的访问情况。

索引此资源:选中该复选框时,Microsoft Index Server 将对该目录进行全文索引,以方便用户快速搜索文档内容。

应用程序设置中，可以设置应用程序名、执行权限、应用程序池。

应用程序名：相应的应用程序名称，改名称将出现在所有包含该应用程序的目录的选项卡中。“配置”表示设置应用程序的属性。

执行权限：控制应用程序能否在此目录下运行，有三种选择：“无”表示不允许任何程序和脚本运行；“纯脚本”表示是映射到脚本引擎的应用程序可以运行；“脚本和执行程序”表示允许任何应用程序在该目录下运行。

应用程序池：用于决定应用程序是否在分开的内存中运行。

③“性能”属性

可以对 Web 站点提供服务的能力做出限制，以合理使用整个服务器的资源，主要有：

带宽限制：如果在服务器上设置多个 Web 站点，就必须根据实际情况限制每个站点使用的带宽，避免出现死机情况。

网站连接：表示同时允许进行连接的网站数目。

④“文档”属性

启动默认内容文档：当用户通过浏览器访问 Web 站点时，如果并未指定具体的文档，这时候服务器就会自动打开默认的文档。主要有 HTML 文件和 ASP 文件两种。

选择“启动默认内容文档”复选框，就能够响应用户的请求。单击“添加”按钮向列表中添加默认文档，并且根据需要调整文档的先后顺序。第一个文档为最优先。

启用文档页脚：选择“启用文档页脚”复选框，可以在该站点下的所有页面上加入一个页脚。单击“浏览”按钮，则指定一个页脚文件的路径。

⑤“目录安全性”属性

选择“身份验证和访问控制”中的“编辑”按钮，弹出如图 6-49 所示的对话框，在该对话框中可以设置启用匿名访问或设置匿名访问使用的用户名和密码，可以在 Active Directory 用户和计算机中选择相应的权限。另外还可以设置以什么样的身份验证方法来访问页面。

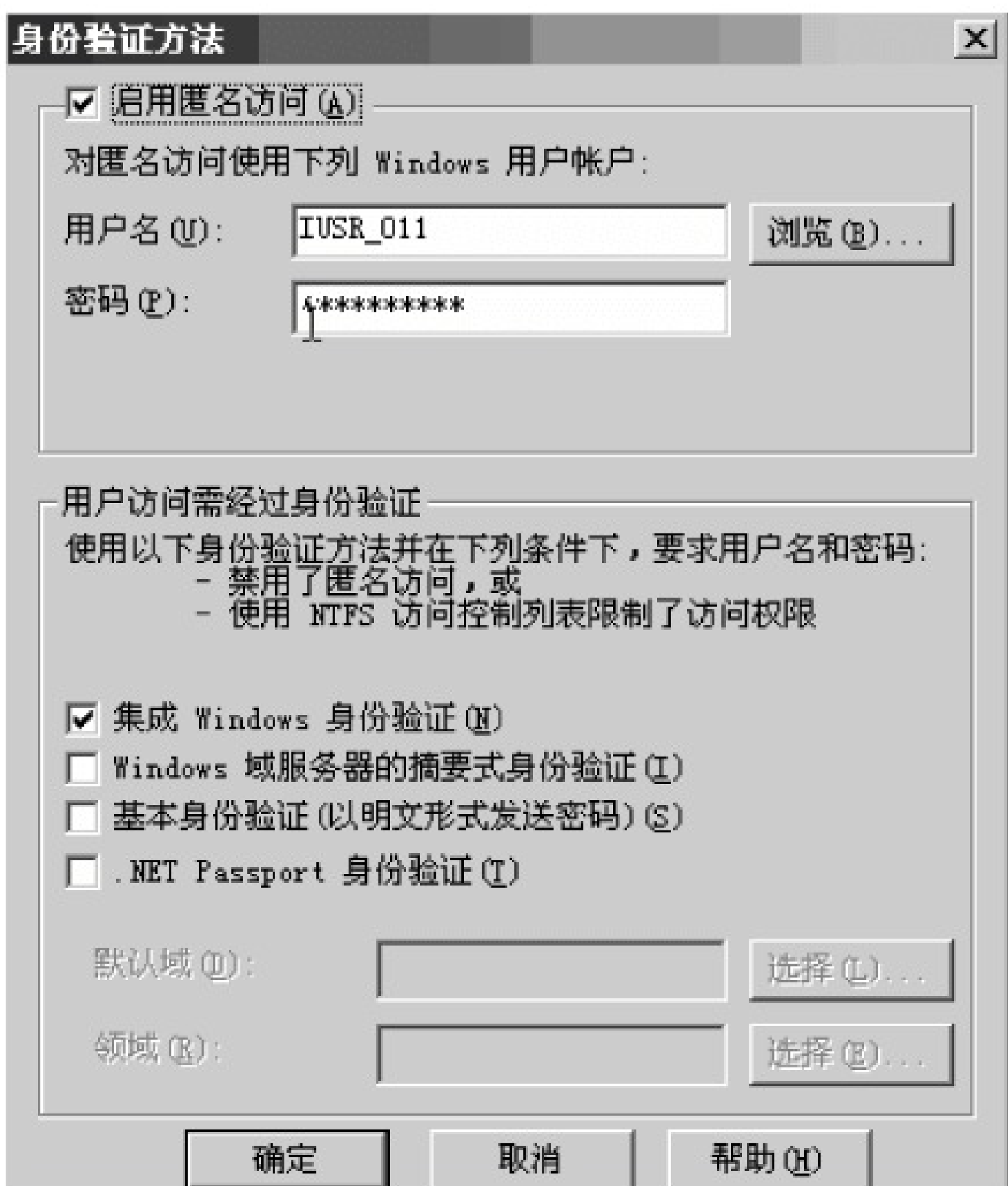


图 6-49　身份验证方法设置

IP 地址及域名限制：该选项可对具体的 IP 地址或域名做出具体的访问时授权或者访问时限制。单击“编辑”按钮，显示“IP 地址及域名限制”对话框，选择“授权访问”或“拒绝访问”，将授权或拒绝所有的 IP 地址或域名访问，另外有新的 IP 地址或域名添加进来，可以单击“添加”按钮。

安全通信：在该选项中创建 SSL 密钥对和服务器证书并将它们绑在一起，这一操作必须在服务器的 IIS 控制台完成，目的是保护 Web 服务器的安全通信。

⑥ “HTTP 头”属性

“启用内容过期”选项：可进一步设置此站点内容过期的时间，当用户浏览此站点时，浏览器会对比当前日期和过期日期，来决定显示硬盘中的网页暂存文件，或是向服务器要求更新网页。

“自定义 HTTP 头”选项：经自定义头的信息返还给用户浏览器。

“内容分级”选项：主要对一些网页内容进行分级，以方便用户有所选择地浏览网页。

“MIME 类型”选项：MIME 作为 Internet 中邮件服务的扩展，指定服务器返回给用户浏览器的类型。

⑦ “ISAPI 筛选器”属性

可设置 ISAPI 筛选程序，ISAPI 筛选器在处理 HTTP 请求过程中，对事件做出响应的程序，加载于 Web 站点的内存中。

⑧ “自定义错误”属性

可以设置自定义错误信息。在列表中选中一个项目，单击“编辑属性”按钮，可以对该项目进行编辑，包括消息类型和文件。

6.2.3 FTP 服务器的配置

任务描述：在一台安装了 Windows Server 2003 系统的服务器上，存放着某单位的一个文本文件，其他计算机用户如何利用 IIS 服务将这个文件下载下来？

任务分解：外界要下载到该文件，需要在服务器上配置支持文件传输的 FTP 服务。

1. FTP 服务器介绍

文件传输协议 FTP(File Transfer Protocol)是重要的 Internet 协议，也是 Internet 的一个组件，它可以在服务器和客户机之间双向传输文件，即上传和下载。FTP 服务也是采用客户机/服务器模式。客户机和服务器之间建立一个 TCP 连接，通过 TCP 端口进行数据传递，默认情况下 FTP 服务器预置的 TCP 端口号为 21 和 20，其中端口号 21 状态为始终开启，用于传输控制命令；端口号 20 只有在进行数据传输时开启，用于传输数据。

FTP 的工作过程如下：

(1) FTP 客户端向 FTP 服务器端申请建立连接。

(2) FTP 服务器的 21 号端口会监听到来自 FTP 客户端的请求，这时会根据设定的权限，做出应答并且与客户端的控制端口建立连接。

(3) 连接建好后，进行数据传送。客户端打开数据端口，连接到 FTP 服务器的 20 号端口进行传输，当数据传输完成后马上断开连接。

2. 创建 FTP 站点

(1) 设置 IIS 中默认的 FTP 站点

① 执行菜单命令“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”，打开“Internet 信息服务”对话框，展开要设置的服务器。

② 右击“默认 FTP 站点”选项，从弹出的快捷菜单中选择“属性”项。

③ 打开“默认 FTP 网站属性”对话框，在“IP 地址”栏选择 IP 地址，端口号默认“21”。

④ 打开“主目录”选项卡，在“本地路径”的右侧单击“浏览”按钮，选择目标目录，选取

访问权限(读取、写入、记录访问),单击“确定”按钮。

建立 FTP 站点最快的方法就是直接利用 IIS 默认建立的 FTP 站点。把可供下载的相关文档,分别放在该站点默认 FTP 根目录\InterPub\ftproot 下即可。

当 FTP 站点建立完成后,可以在客户端的浏览器中输入 ftp://IP 地址或域名地址,就可以访问 FTP 站点。

(2) 创建 FTP 虚拟目录

创建虚拟目录便于 FTP 网站的结构化管理。虚拟目录可根据需要映射到不同的物理目录,这些目录可位于同一计算机的其他驱动器上,或在网络上的其他计算机上。不论物理目录如何变动,只要使用虚拟目录访问即可。

虚拟目录的建立步骤如下。

在“Internet 信息服务(IIS)管理器”窗口中,右击要添加虚拟目录的 FTP 站点,选择菜单命令“新建”下的“虚拟目录”,在弹出的“虚拟目录向导”对话框中,单击“下一步”按钮。

在打开的“虚拟目录别名”对话框中输入所创建虚拟目录的别名,如图 6-50 所示,单击“下一步”按钮。



图 6-50　“虚拟目录别名”对话框

打开“FTP 网站内容目录”对话框,输入所创建虚拟目录对应的物理目录路径。如果是其他计算机上的共用文件夹,在“路径”文本框中输入“\\服务器\共享名”的网络路径,接着输入用户账号和密码,单击“下一步”按钮。

打开“虚拟目录访问权限”对话框,设置所创建的虚拟目录的访问权限,单击“下一步”按钮。

完成虚拟目录的创建。

建立完网站后,在 IE 浏览器地址栏中输入“ftp://IP 地址(或域名地址)/别名”,即可打开并连接到 FTP 服务器。

(3) 添加或删除站点

IIS 允许在同一台计算机上同时为多个用户创建 FTP 站点。为多个用户创建 FTP 站点,有以下两种方法。

① 一种方法是每个用户建立一个 FTP 站点。如果只有一个 IP 地址,可以为不同的 FTP 站点设置不同的端口号。建议端口号用 10000～65535。当有多个 IP 地址时,不同的 FTP 站点设置不同的 IP 地址,端口号采用默认的“21”。添加步骤:在“Internet 信息服务(IIS)管理器”窗口中,选取“FTP 站点”项,再执行菜单命令“操作”→“新建”→“FTP 站点”,便会运行 FTP 安装向导,向导会要求输入新站点的 IP 地址、TCP 端口、存放文件的主目录路径,以及设置访问权限,如图 6-51 所示。

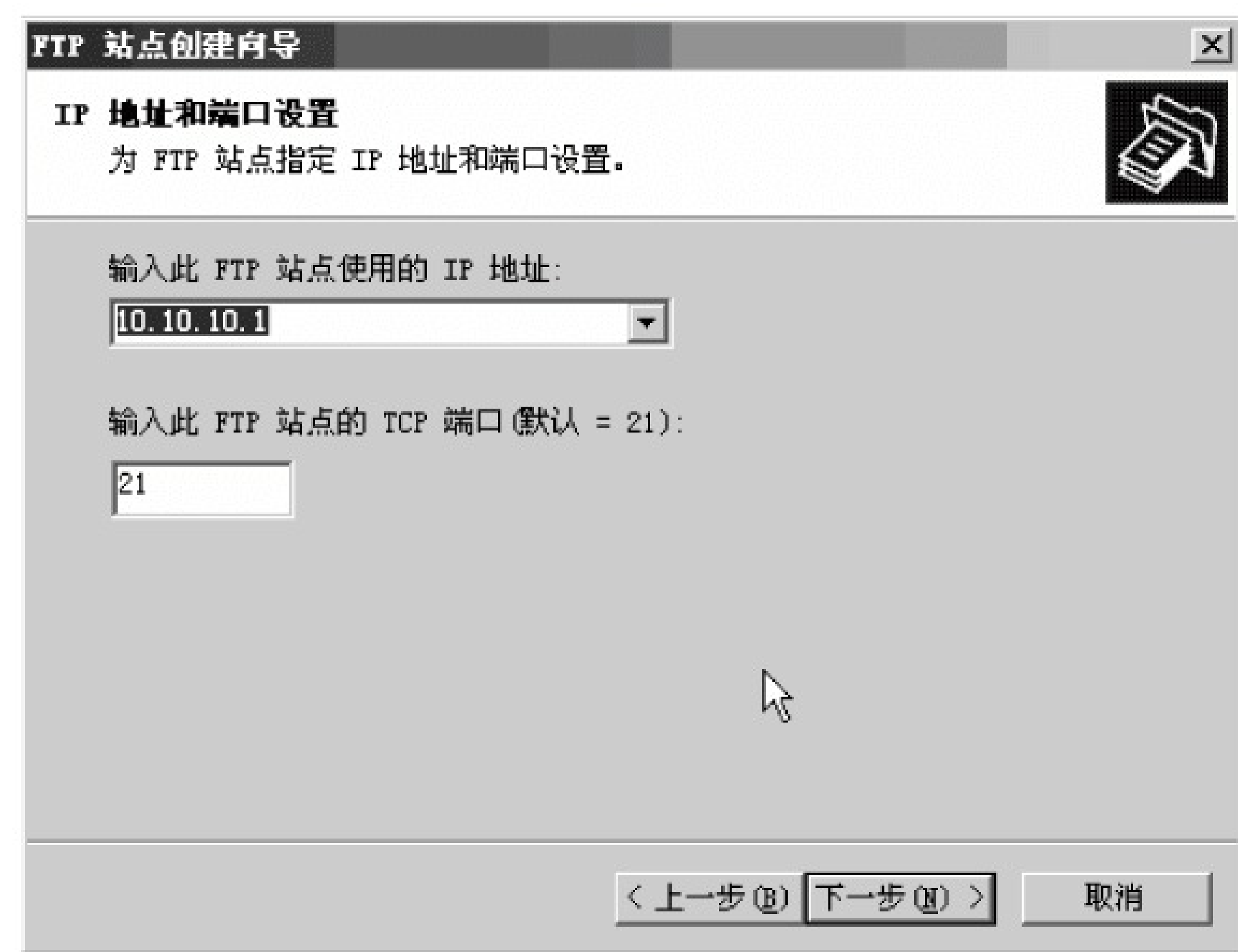


图 6-51　FTP 站点创建向导

如果站点是采用的不同的端口号,访问时必须以“ftp://IP 地址(或域名地址):端口号”的形式访问。

删除 FTP 站点,先右击要删除的站点,再执行“删除”命令即可。如果一个站点被删除,只是该站点的设置被删除,而该站点下的文件还是存放在原先的目录中,并不会被删除。

② 另一种方法为所有用户建立一个 FTP 站点,然后在站点下面为每一个用户建立自己的主目录。为保证每个用户主目录的安全性,可以将用户隔离,让其只能访问自己的主目录文件夹。

具体操作步骤如下。

建立 FTP 站点。FTP 站点的建立过程和前种方法相同,输入对应的 IP 地址、端口号 21,路径(所有用户个人目录的上级目录),权限为写入,只是在 FTP 隔离用户时选择“隔离用户”,如图 6-52 所示。

建立用户账户。为每一个访问 FTP 站点的用户在活动目录或计算机管理中建立自己的用户账户,并设置密码。默认情况下,用户账户没有密码是不能访问 FTP 服务器的。

建立 FTP 用户的主目录。在 FTP 的根目录下,建立与用户账户同名的主目录。

如果没有为用户建立同名的文件夹,用户将不能登录到 FTP 服务器。

设置完成后,当用户登录时就会自动进入自己的主目录。由于用户没有进入其他用户主目录的权限,可以保证其他用户文件的安全。

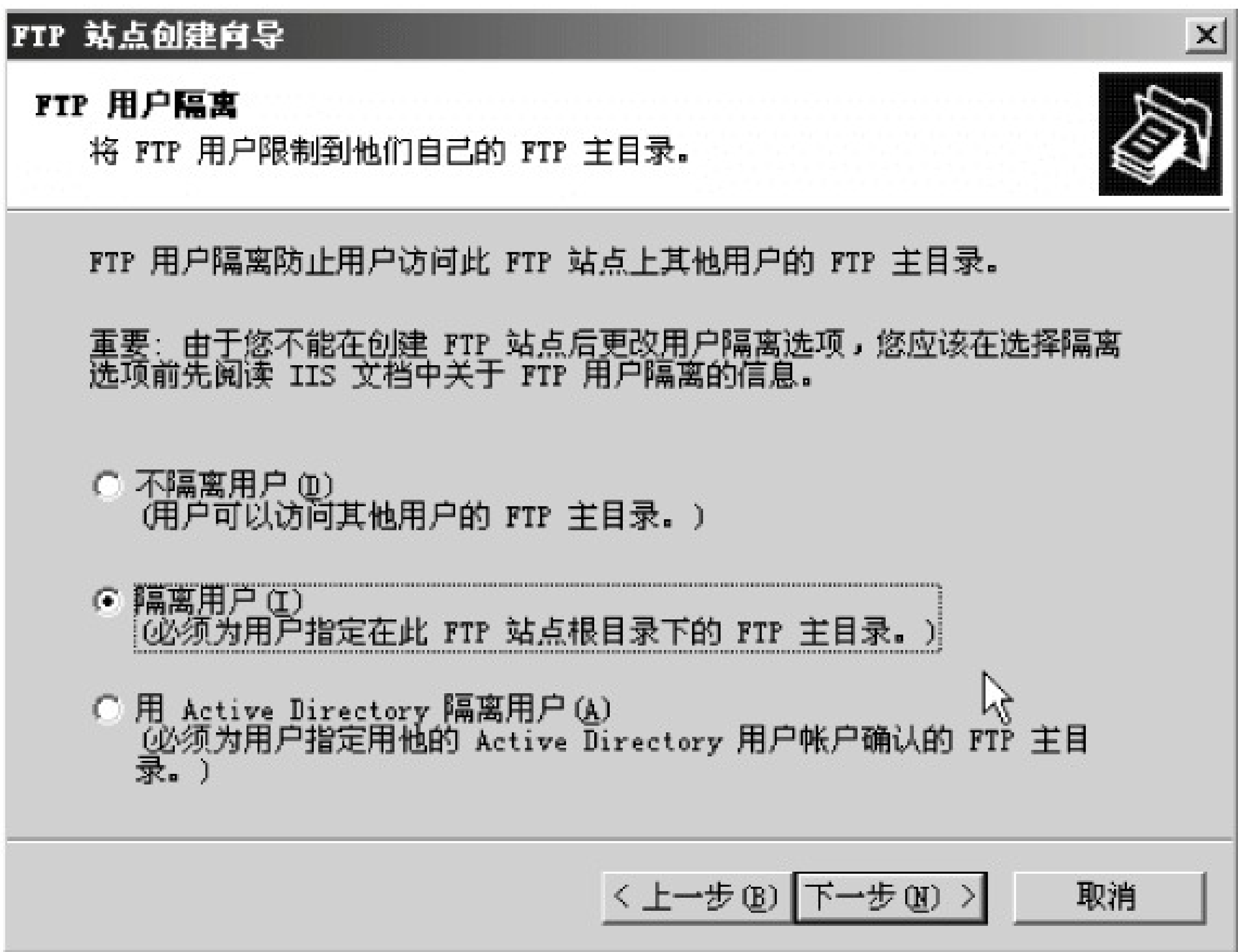


图 6-52　IP 用户隔离

3. FTP 站点的管理

FTP 站点建立好之后，可以通过“Internet 信息服务(IIS)管理器”窗口进一步来管理和设置 FTP 站点，站点管理工作既可以在本地进行，也可以远程管理。

打开“Internet 信息服务(IIS)管理器” 窗口，右击要管理的 FTP 站点，选择“属性”命令，出现如图 6-53 所示的对话框。

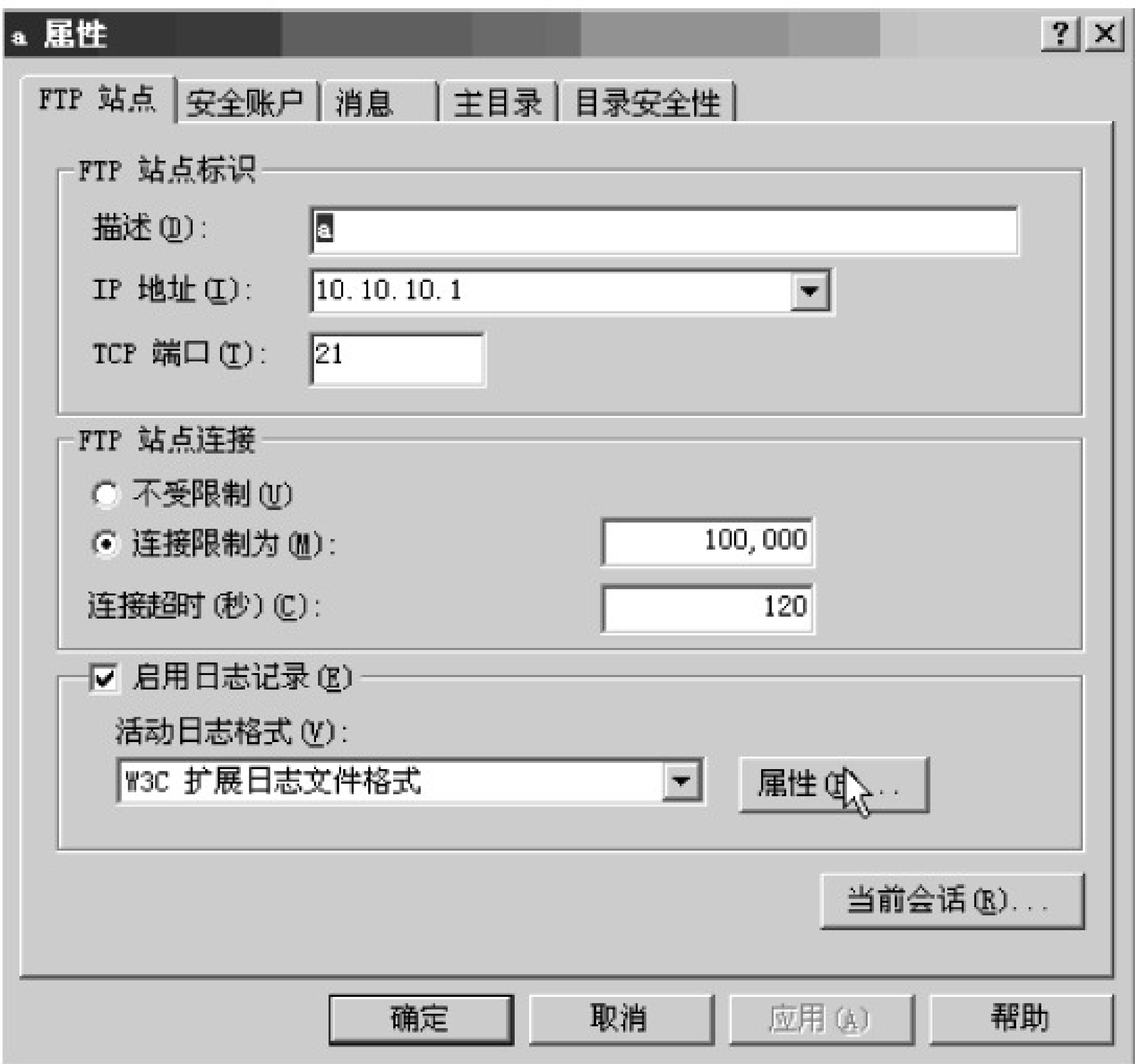


图 6-53　“FTP 站点”属性

(1)“FTP 站点”属性

IP 地址：设置站点的 IP 地址，即 FTP 服务器的地址。

TCP 端口：FTP 服务器与客户端连接时的端口号，默认情况下是 21，用户也可以更改。

FTP 站点连接、启用日志文件的设置参见 Web 服务器的设置。

(2)“安全账号”属性

允许匿名连接：FTP 站点在一般情况下，允许用户进行匿名访问。FTP 系统安装时自动建立一个匿名账号，而用户在使用客户机登录时使用的匿名用户名是 annonymous。

只允许匿名连接：用户不能使用自己的用户账号登录，只能用匿名的账号登录，目的是防止具有高级管理权限的账号通过 FTP 访问或更改文件。

(3)“消息”属性

在该选项中，可以设置一些用户登录后看到的站点公告的信息。

(4)“主目录”属性

资源内容来自于：此计算机上的目录或者另一台计算机上的共享资源。

选择此计算机上的目录后，还需指定 FTP 站点目录；选择另一台计算机上的共享资源，需指定来自于其他计算机的目录。

对于站点的访问权限设置，包括“读取”、“写入”、“记录访问”。

(5)“目录安全性”属性

授权访问：对所有的用户开放访问权限，可在“下列地址例外”列表中选择不受欢迎的用户 IP 地址。

拒绝访问：所有的用户都不能访问该站点，可在“下列地址例外”列表中选择允许访问的用户 IP 地址。

6.2.4 DHCP 服务器的配置

任务描述：要组建一个小的局域网，在服务器上安装 Windows Server 2003，其余 20 台计算机作为客户机使用，如何使用动态分配 IP 地址的方式，将它们组成一个局域网？

任务分解：在服务器上安装 DHCP 服务，并进行适当配置，实现动态分配 IP 地址。

1. DHCP 服务介绍

DHCP 是动态主机配置协议(Dynamic Host Configuration Protocol)，它能集中管理和分配 IP 地址，并且对用户的 TCP/IP 协议进行配置。

给客户机分配 IP 地址的两种方式如下。

静态 IP 地址：又称为手工分配，给每台主机指定一个固定的 IP 地址。

动态 IP 地址：由 DHCP 服务器动态地给主机分配 IP 地址，即 DHCP(动态主机配置协议)，DHCP 服务工作模式为客户机/服务器模式，DHCP 服务器利用租约的方式为客户机分配 IP 地址，这种租约的方式有一定的租约期限，定义了指派的 IP 地址可以使用的时间长度。租约期默认为 8 天，也可以自行设置。当一个 DHCP 客户机启动时，它就从 DHCP 服务器请求一个 IP 地址。当 DHCP 服务器接收到该请求时，它就从数据库定义的地址范围中选择一个 IP 地址，分配给客户机。

2. DHCP 服务的安装

(1) 运行 DHCP 服务的前提要求

DHCP 客户在登录的时候，DHCP 服务器会从可用的 IP 地址中动态地将一个地址分配给 DHCP 客户，当 DHCP 注销时，该 IP 地址又会被收回，等待下一次分配，每次分配

给客户的 IP 地址是不相同的。

DHCP 服务器有如下要求：

DHCP 服务必须安装在 Windows Server 2003 上。

DHCP 服务器必须有一个静态的 IP 地址。

要使用 DHCP 服务，必须在 DHCP 服务器中创建 DHCP 作用域，分配给 DHCP 服务器一组 IP 地址。

DHCP 客户端有如下要求：

对客户端的计算机进行配置，在 TCP/IP 属性中设置为自动获得 IP 地址。

（2）DHCP 服务的安装

① 执行菜单命令“开始”→“设置”→“控制面板”，单击“删除/添加程序”图标，选择“删除/添加 Windows 组件”项。

② 在对话框中，选中“网络服务”复选框，单击“详细信息”按钮，选择“动态主机配置协议（DHCP）”复选框，单击“确定”按钮，再单击“下一步”按钮，最后单击“完成”按钮。

需要提供 Windows Server 2003 的安装光盘。

③ 执行菜单命令“开始”→“程序”→“管理工具”，右击 DHCP 图标，可以选择启动 DHCP 服务。

（3）对 DHCP 服务授权

安装了 DHCP 服务后，在使 DHCP 服务器正确地运行之前，须对 DHCP 服务器进行授权。

对 DHCP 服务器进行授权的操作步骤如下：

① 以 Administrator 的身份登录。

② 打开“管理工具”中的 DHCP 项，出现如图 6-54 所示的 DHCP 窗口。

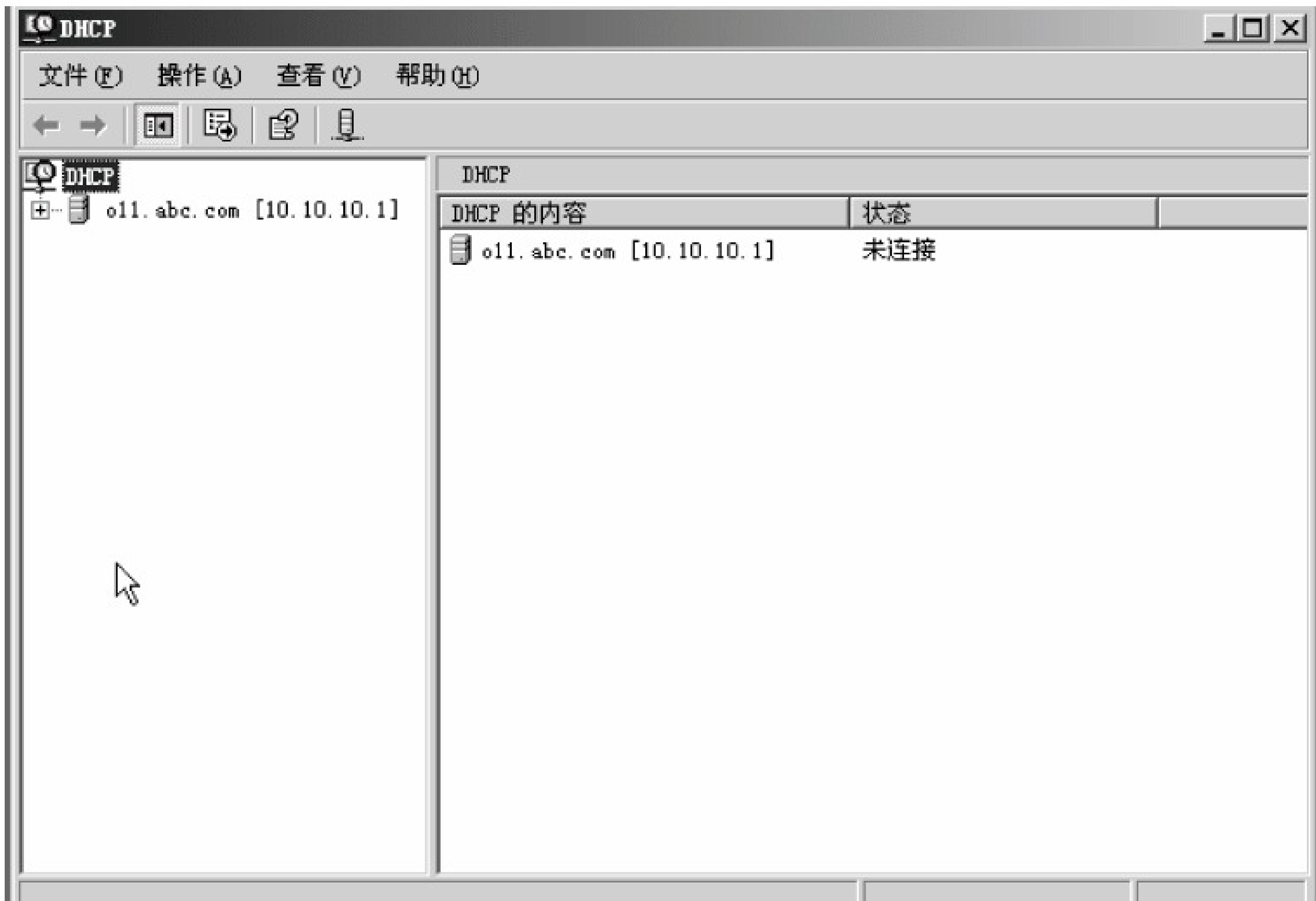


图 6-54　DHCP 窗口

③ 在如图 6-54 所示的 DHCP 窗口中，执行菜单命令“操作”→“管理授权的服务器”，出现如图 6-55 所示的对话框。

④ 单击“授权”按钮，出现如图 6-56 所示的对话框。

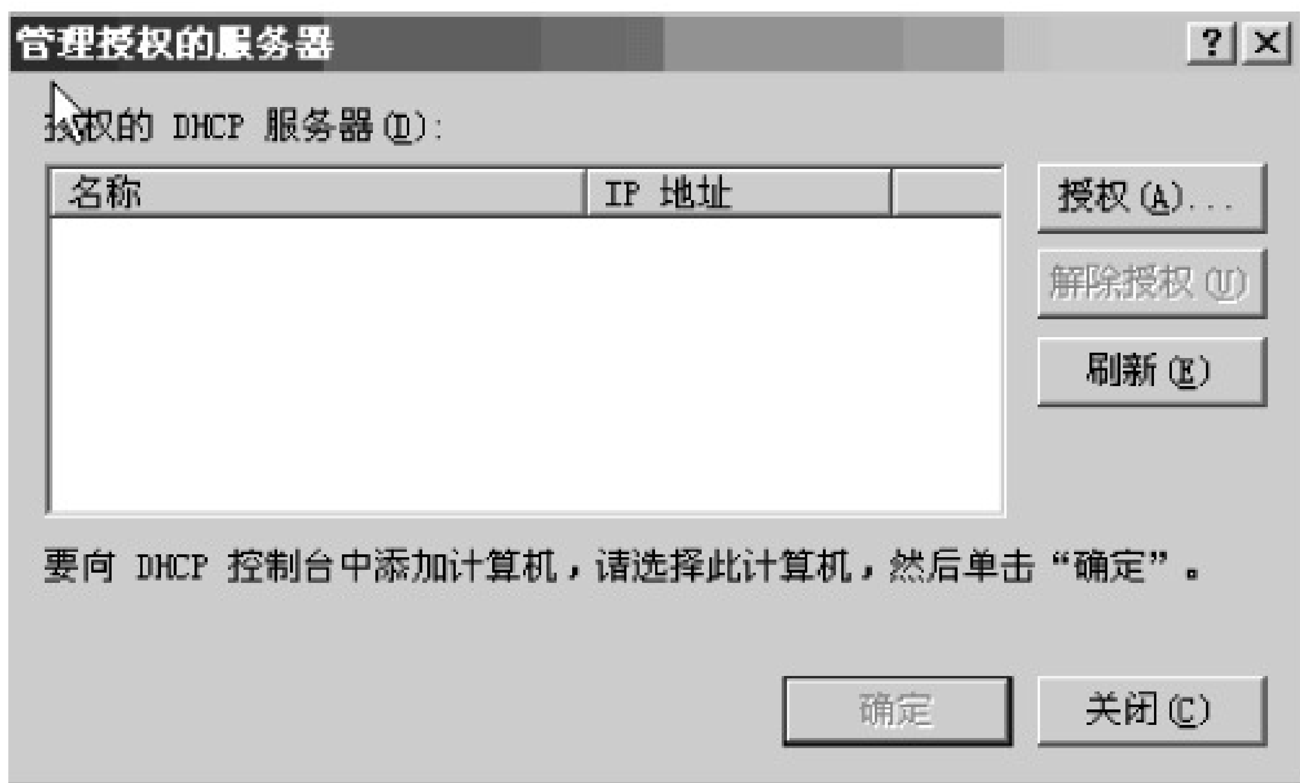


图 6-55 “管理授权的服务器”对话框

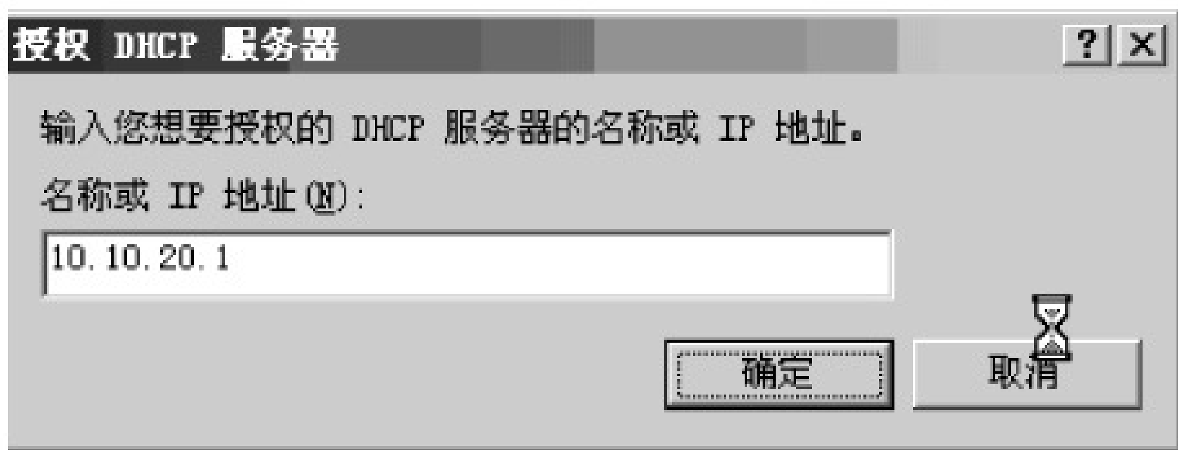


图 6-56 “授权 DHCP 服务器”对话框

⑤ 单击“下一步”按钮，根据提示信息，单击“是”按钮，完成对 DHCP 服务器的授权。

若要解除授权的 DHCP 服务器，只需要在如图 6-55 所示的对话框中，选择授权的 DHCHP 服务器，单击“解除授权”按钮即可。

(4) DHCP 服务器作用域

要想完成分配 IP 地址任务，必须有一组被允许分配的 IP 地址。然后通过 DHCP 服务器根据用户的租约请求将这些地址发布。作用域实际上就是一组有效的 IP 地址，用户通过配置 DHCP 服务器上的作用域确定服务器可分配给客户端的 IP 地址池。当客户端发出申请，DHCP 服务器就可从作用域中选择可使用的 IP 地址，将其分配给客户端。

每一个 DHCP 服务器上至少要有一个作用域，也可以创建多个作用域。但是每个子网只能建立一个作用域，如果希望分配的 IP 地址不连续，则必须建立大于可能使用地址的最大范围的作用域。

建立作用域的步骤如下。

① 在 DHCP 对话框中，右击该 DHCP 服务器，在弹出的快捷菜单中单击“新建作用域”项，出现如图 6-57 所示的对话框，单击“下一步”按钮。

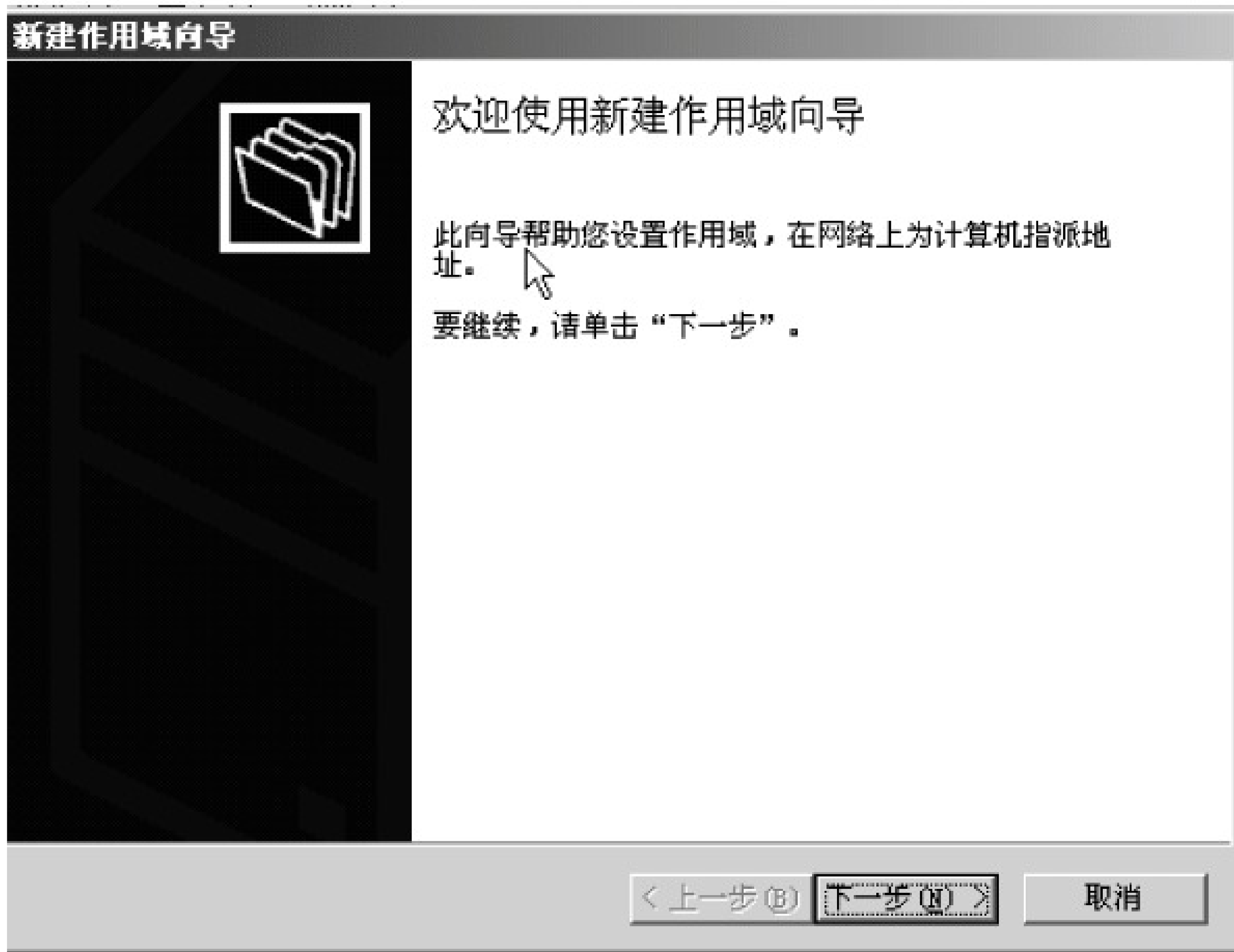


图 6-57 “新建作用域向导”对话框

② 在如图 6-58 所示对话框的“名称”文本框中输入名称，在“描述”文本框中输入说明，然后单击“下一步”按钮。

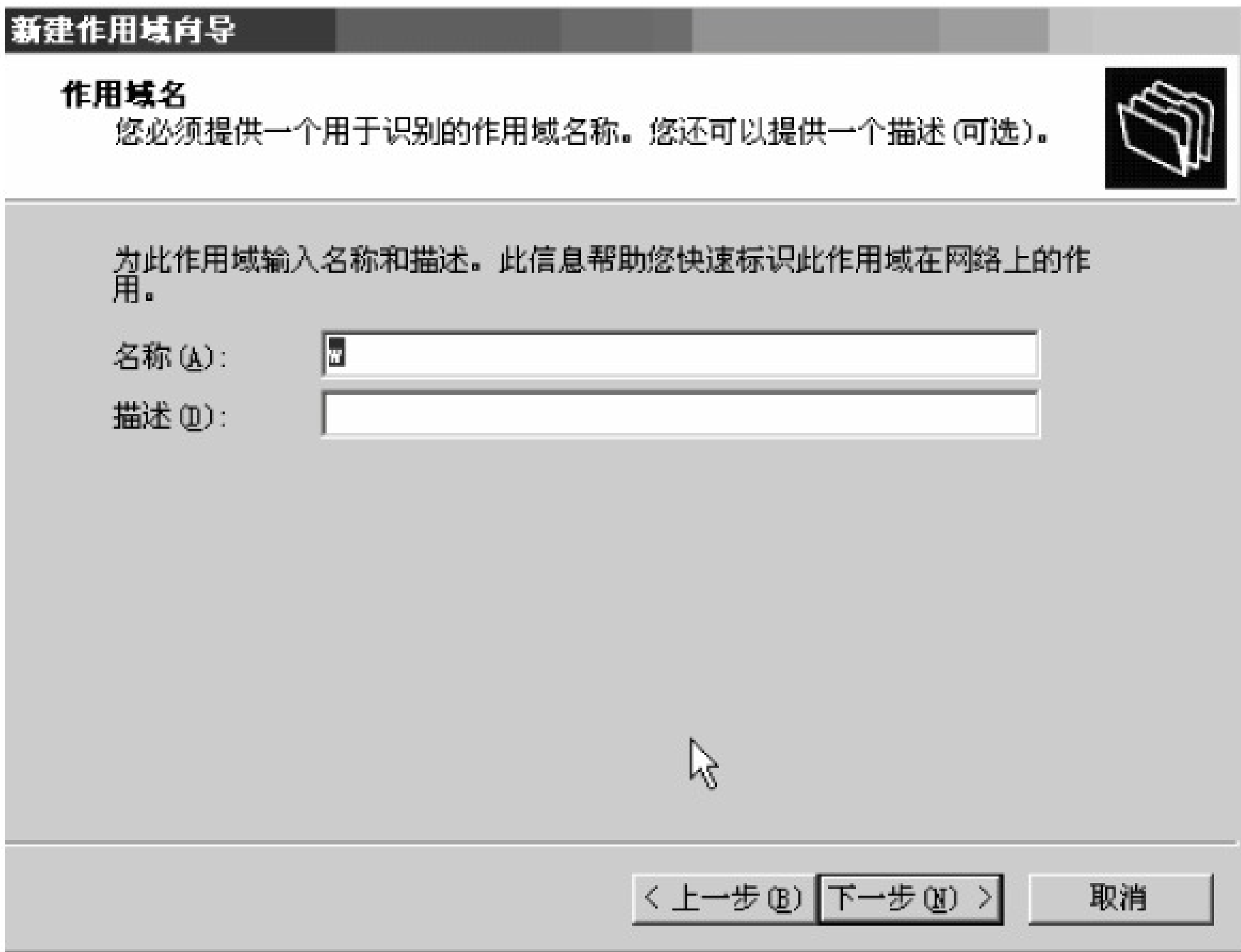


图 6-58　“作用域名”对话框

③在弹出的如图 6-59 所示的界面中输入 DHCP 服务器分配的起始 IP 地址、结束 IP 地址和设置这些地址的子网掩码，单击“下一步”按钮。

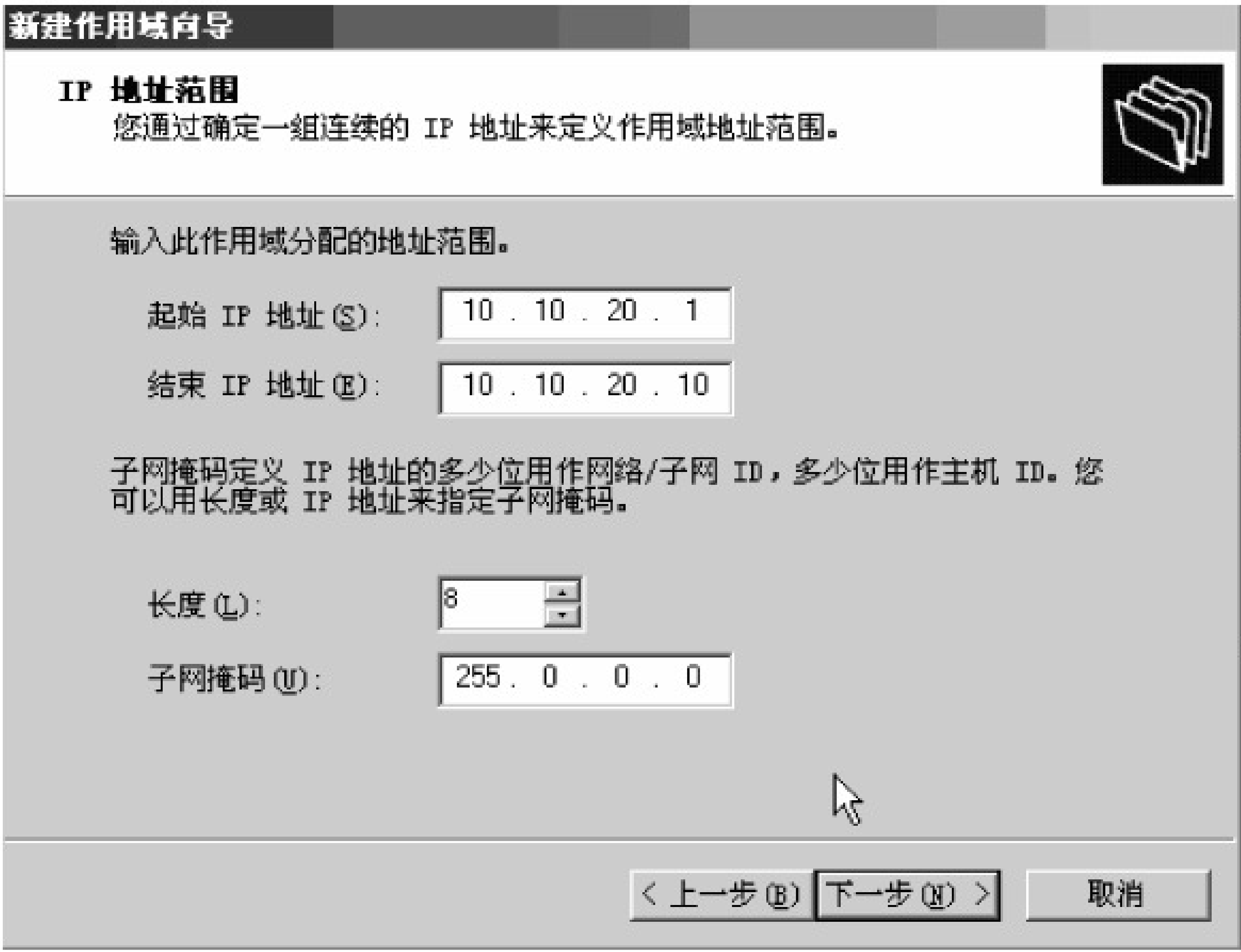


图 6-59　IP 地址范围

④ 在弹出的如图 6-60 所示的对话框中，如果在 IP 作用域中有些 IP 地址不能分配给 DHCP 的客户端，输入需要排除的 IP 地址范围，单击“添加”按钮。设置完排除范围之后，单击“下一步”按钮。

⑤ 在弹出的如图 6-61 所示的对话框中设置 IP 地址的租约期限，默认值为 8 天，设置完租约期限后，单击“下一步”按钮。

⑥ 在如图 6-62 所示的对话框中选择“是，我想现在配置这些选项”单选按钮，单击“下一步”按钮，弹出输入默认网关(路由器地址)对话框，如图 6-63 所示。

⑦ 如图 6-63 所示输入网关地址后，单击“添加”按钮，然后单击“下一步”按钮。

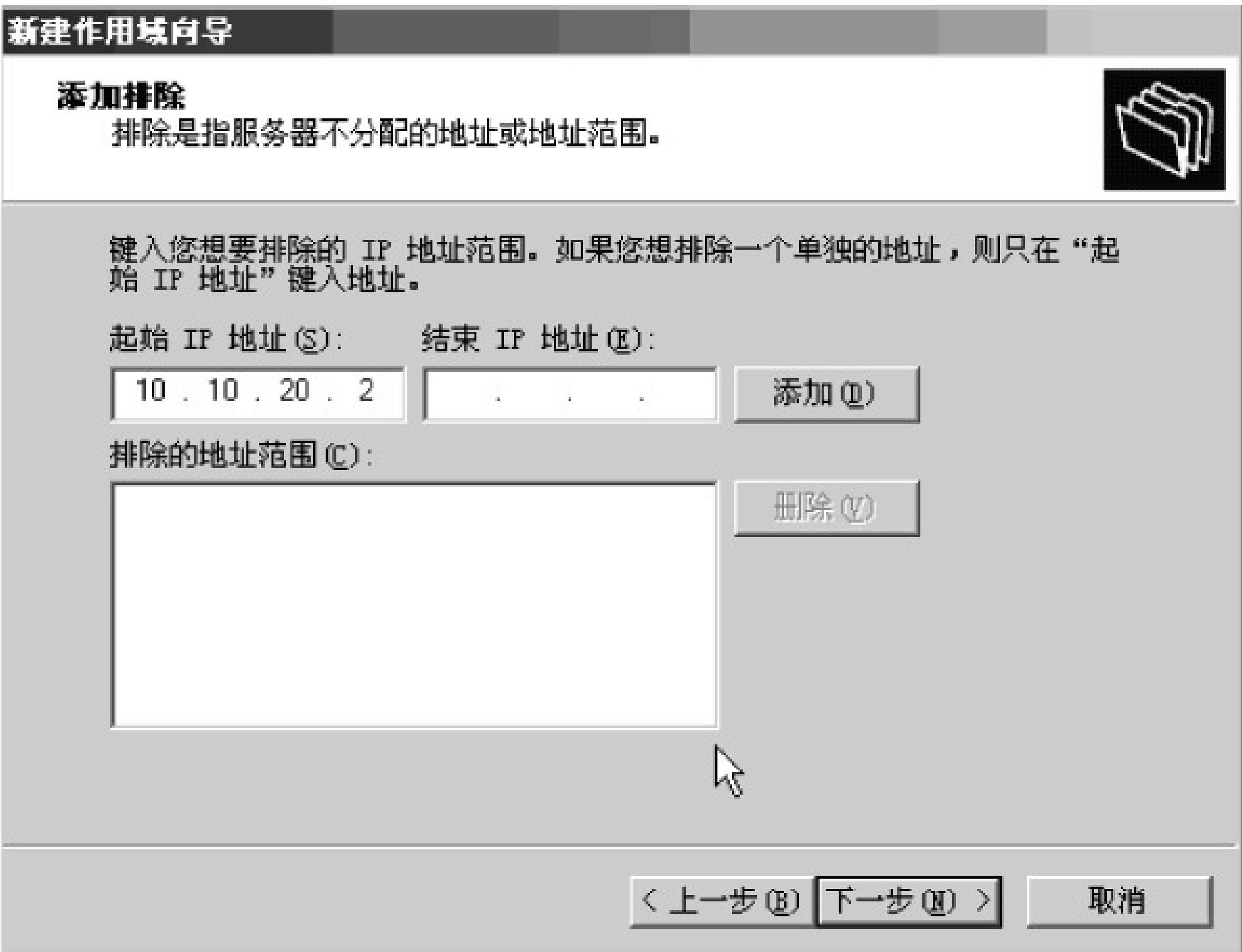


图 6-60　添加排除 IP 地址范围

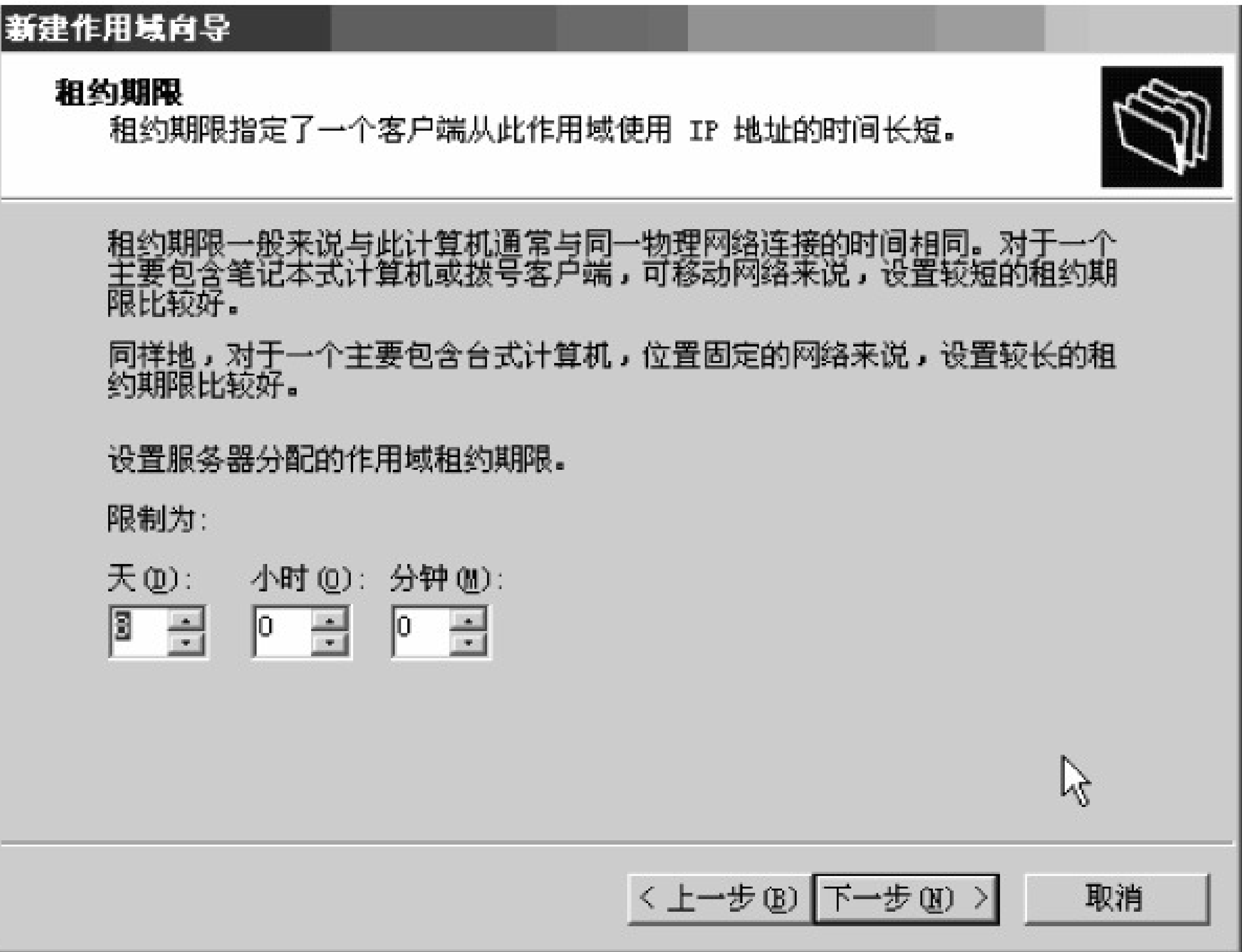


图 6-61　租约期限

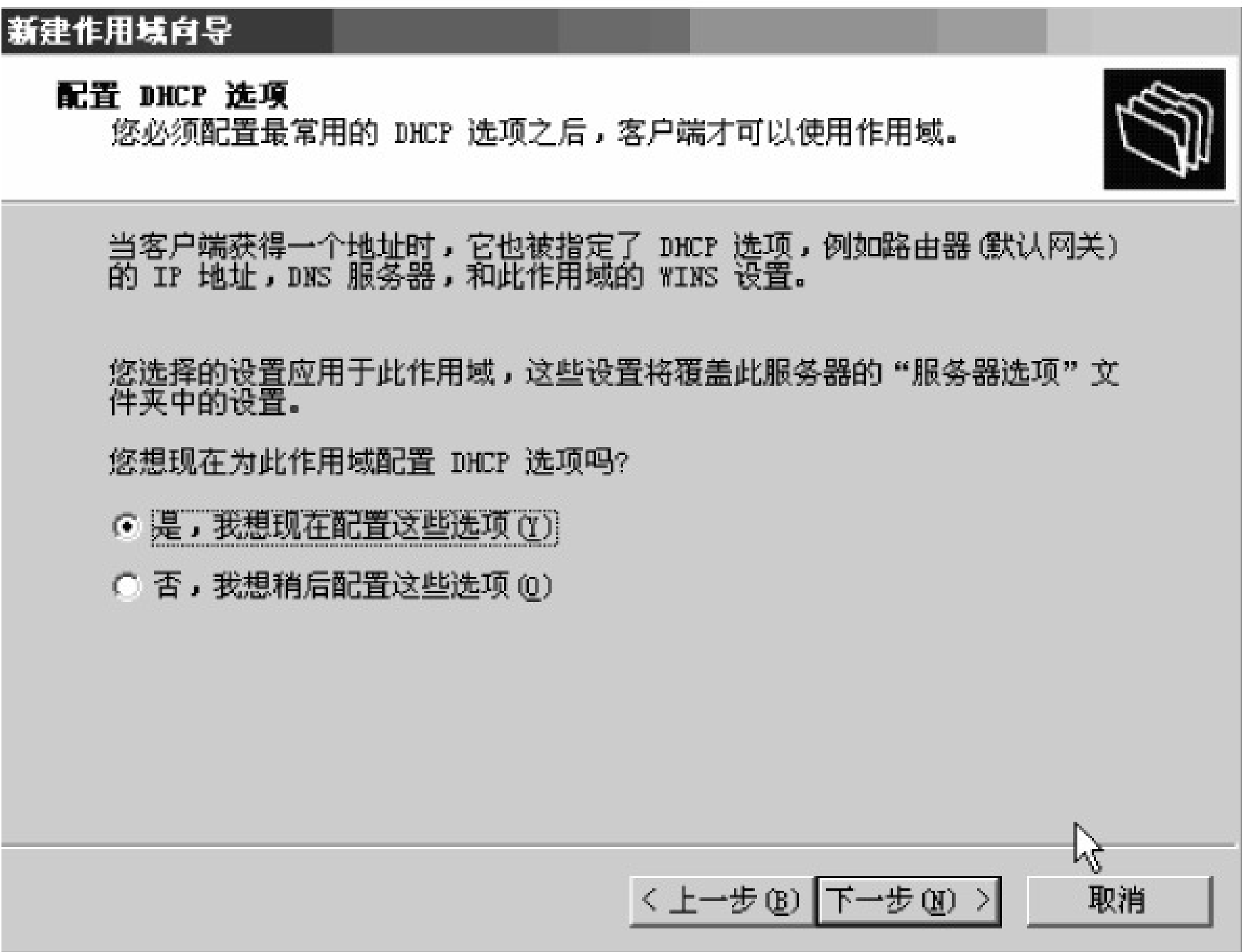


图 6-62　配置 DHCP 选项

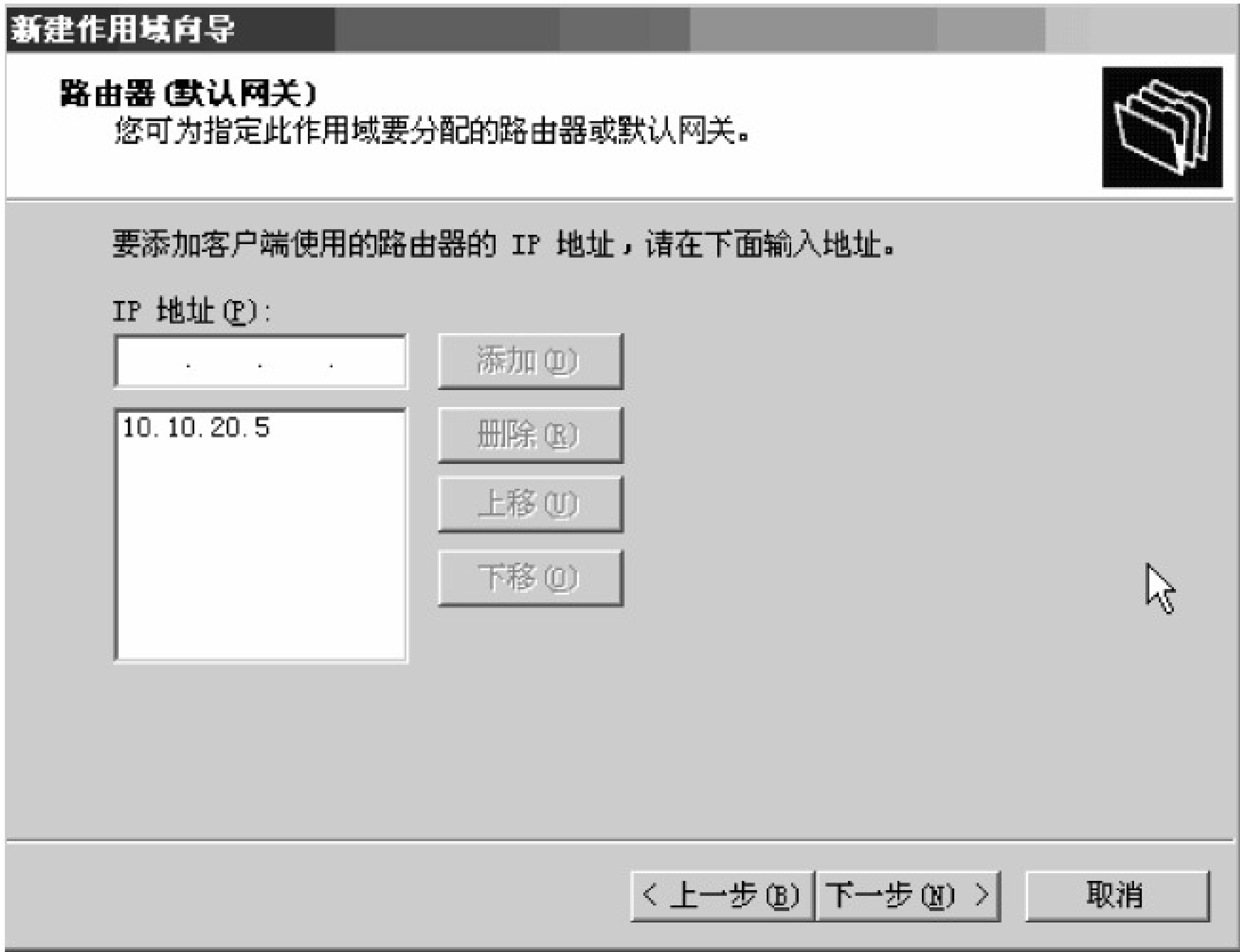


图 6-63　路由器对话框

⑧ 在如图 6-64 所示界面中输入父域和服务器名称后，单击“解析”按钮，“IP 地址”文本框中出现其服务器 IP 地址，然后单击“添加”按钮，再单击“下一步”按钮。

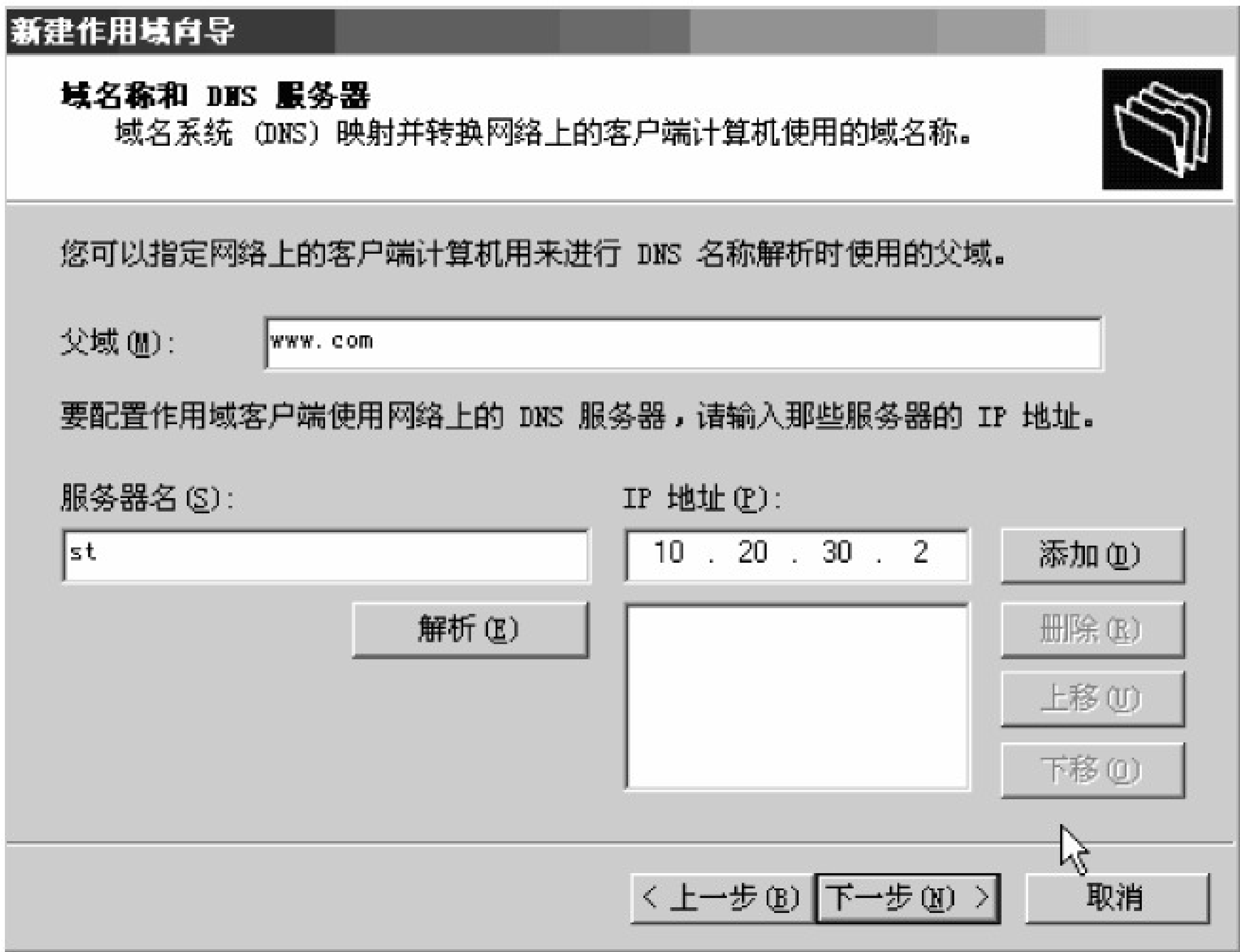


图 6-64　“域名称和 DNS 服务器”对话框

⑨ 弹出如图 6-65 所示界面，若需要安装 WINS 服务器，则输入 WINS 服务器的名称后，单击“解析”按钮，“IP 地址”文本框中出现其服务器 IP 地址，然后单击“添加”按钮。若没有就单击“下一步”按钮，再单击“下一步”按钮。

⑩ 在如图 6-66 所示界面中选择“是，我想现在激活此作用域”单选按钮，单击“下一步”按钮。单击“完成”按钮就完成了 DHCP 作用域的创建了。

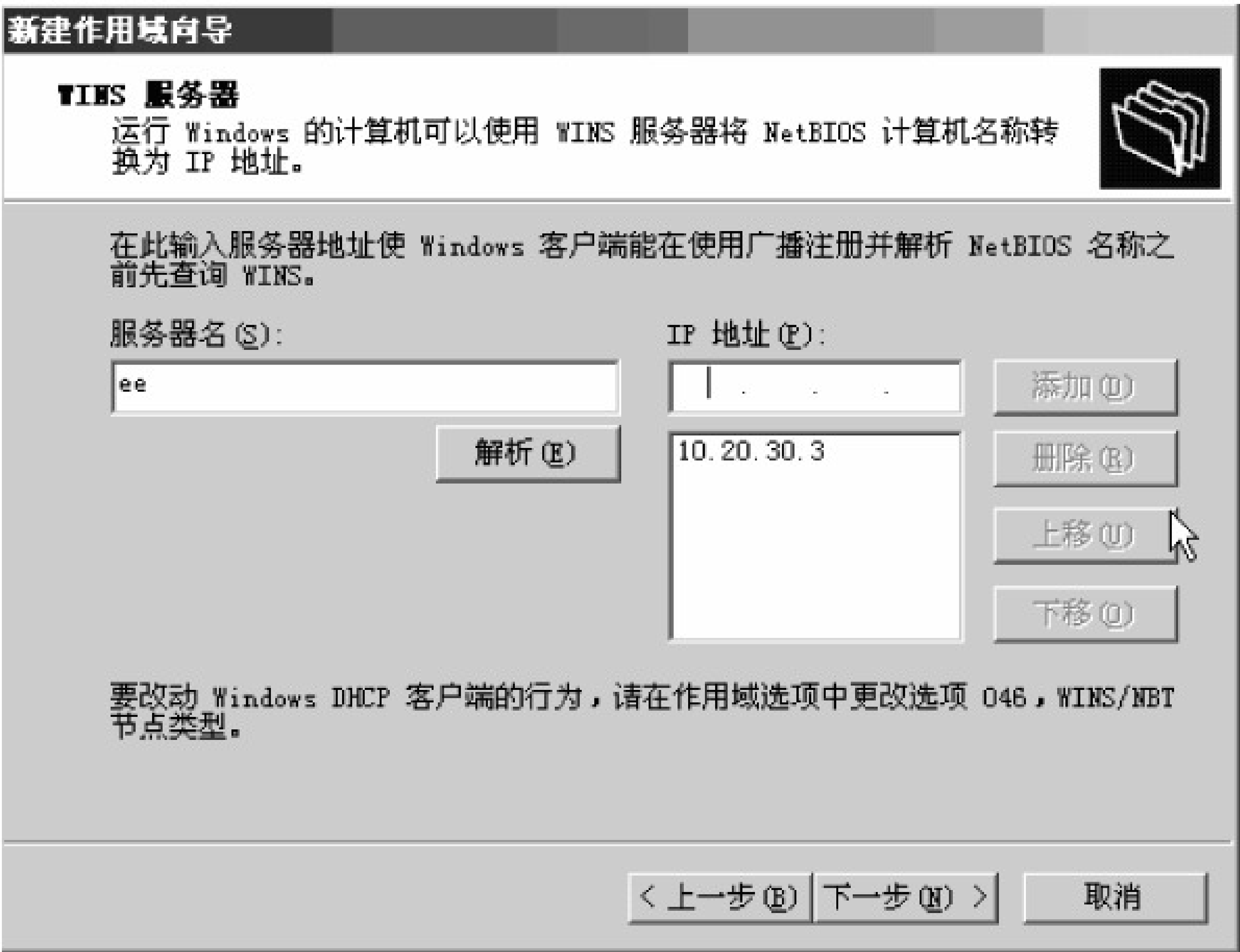


图 6-65 “WINS 服务器”对话框

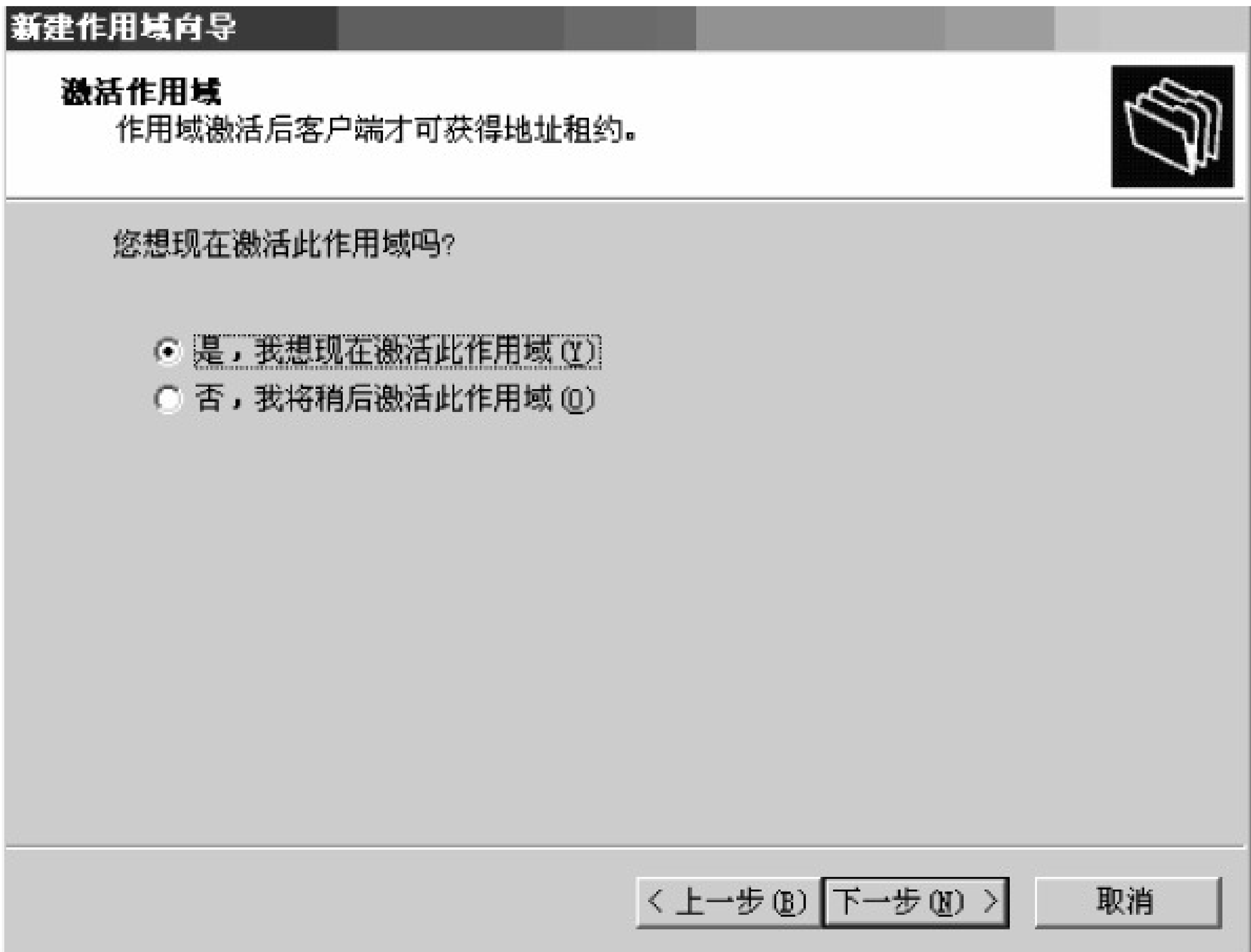


图 6-66 “激活作用域”对话框

6.2.5 邮件服务器的配置

任务描述：电子邮件是网络用户主要的通信方式，实现局域网内邮件的发送与接收。

任务分解：要实现邮件服务支持，需要安装邮件服务器，并进行相应的配置。

1. 邮件服务器的安装

简单邮件传输协议 SMTP 是 Internet 上使用最多的邮件传送协议。Windows Server 2003 中增强了它的功能，而且在安全性能方面也有很大的提高。

邮件协议 POP3 规定了怎样将个人计算机连接到 Internet 的邮件服务器和下载电子邮件的电子协议。它是 Internet 电子邮件的第一个离线协议标准，它允许用户从服务器上把邮件存储到本地主机上，同时删除保存在邮件服务器上的邮件，而 POP3 服务器是遵守 POP3 协议的接收邮件服务器，用来接收和存储电子邮件。POP3 在处理客户端和服务器的连接时，有三种处理状态：认证状态、处理状态和更新状态。

认证状态。客户端在接收邮件前先要接收邮件服务器的验证，如果它发送的用户名和密码与服务器上的匹配，就会进入到处理状态，如果不匹配，客户端会收到一条出错信息，并且无法连接以收取邮件。

处理状态。客户端向服务器发送 POP3 命令，服务器根据 POPE 接收并响应，如果命令不能被 POP3 解释，则会给客户端发送一条出错信息。

更新状态。客户端与服务器断开连接。断开连接后，在服务器上被客户端收取的邮件被标志并被删除，除非客户端要求在服务器上保存副本。

安装 SMTP、POP3 服务的步骤如下：

执行菜单命令“开始”→“控制面板”，选择“添加或删除程序”图标，打开“添加或删除程序”窗口。

(1) 在窗口中，选择“添加/删除 Windows 组件”项，打开“Windows 组件向导”窗口。

(2) 选择“应用程序服务器”复选框，单击“详细信息”按钮，弹出“应用程序服务器”窗口，选择“Internet 信息服务(IIS)管理器”窗口。

(3) 在“Internet 信息服务(IIS)管理器”窗口中，选择 SMTP Service 复选框，单击两次“确定”按钮。

(4) 在“Windows 组件向导”窗口中，选择“电子邮件服务”复选框，单击“详细信息”按钮，打开“电子邮件服务”对话框。

(5) 在窗口中选择“POP3 服务”和“POP3 服务 Web 服务”复选框，单击“确定”按钮，然后单击“下一步”按钮，按提示完成 SMTP、POP3 服务的安装。

2. POP3 的配置

当服务器的配置完成后，就要为用户建立邮件域名，然后在邮件域中建立邮箱。

(1) 建立邮件域

① 执行菜单命令“开始”→“管理工具”→“POP3 服务”，打开“POP3 服务”管理窗口。其窗口如图 6-67 所示。

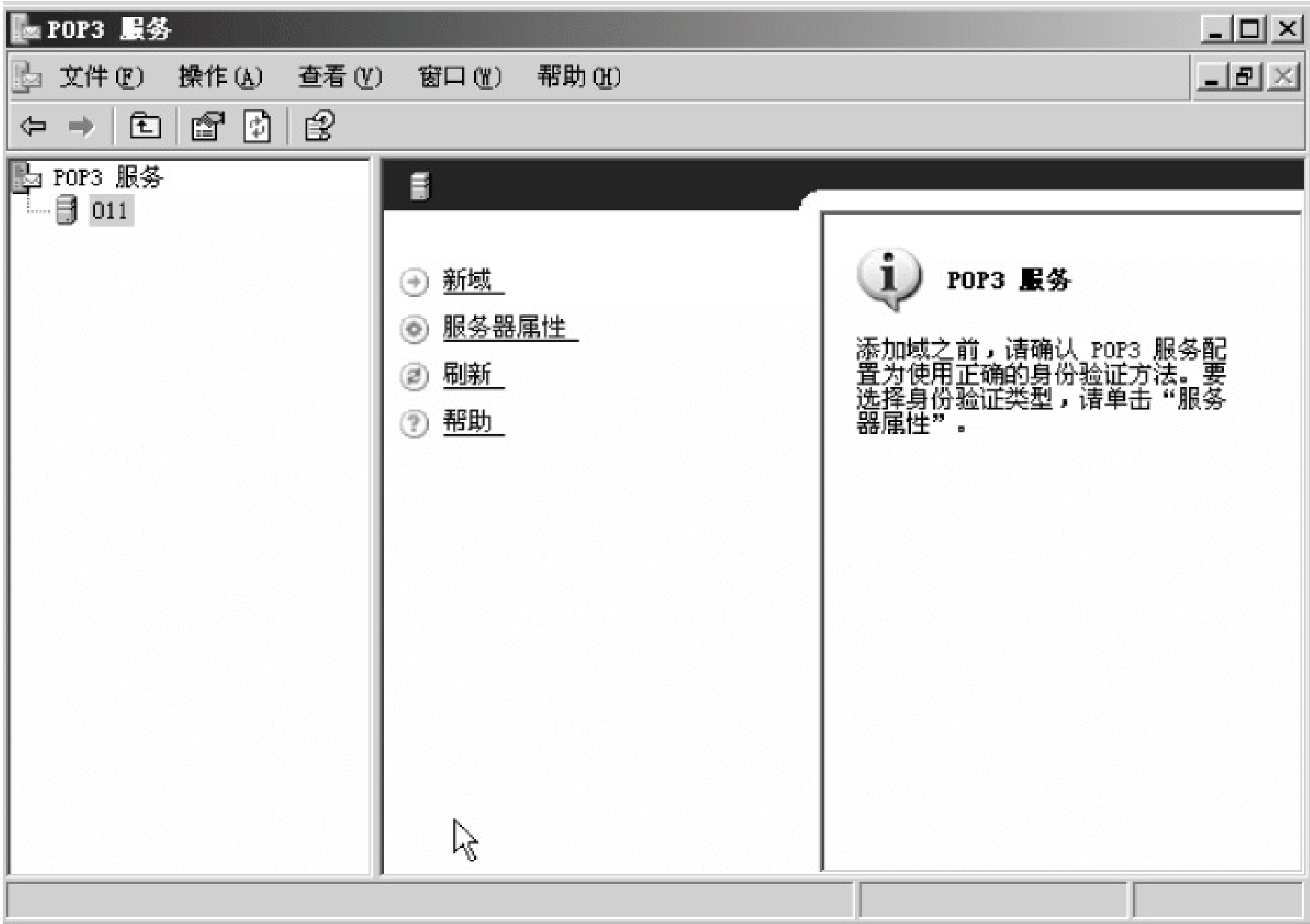


图 6-67 POP3 服务

② 用鼠标右击你的服务器，从弹出的快捷菜单中选择“新建”项下的“域”，打开“添加域”对话框。在“域名”文本框中输入要新建的域名，然后单击“确定”按钮。

POP3 服务支持顶级到三级的域名。建立好邮箱的域以后，可在里面为用户建立邮箱。

③ 在“POP3 服务”对话框中，展开本机名称，再单击你建立的域名。在窗口右侧单击“添加邮箱”链接，如图 6-68 所示。



图 6-68　建立新邮箱

④ 打开“添加邮箱”对话框。输入邮箱名、密码、确认密码，单击“确定”按钮。

⑤ 弹出“成功添加了邮箱”的提示框，单击“确定”按钮，关闭此对话框。

⑥ 用同样的方法建立其他邮箱。新建邮箱后，可在控制台窗口的右侧看到邮箱列表，包括邮箱名、当前邮箱大小、当前邮箱内的消息数以及邮箱的状态。

(2) 管理邮箱空间

默认情况下，邮箱的空间不受限制。可以利用 NTFS 文件系统配额功能和 WINPOP 命令来限制邮箱的空间。

具体操作方法如下。

① 右击 NTFS 格式的磁盘，选择快捷菜单中的“属性”项，打开“本地磁盘(C:)属性”对话框，打开“配额”选项卡，如图 6-69 所示。

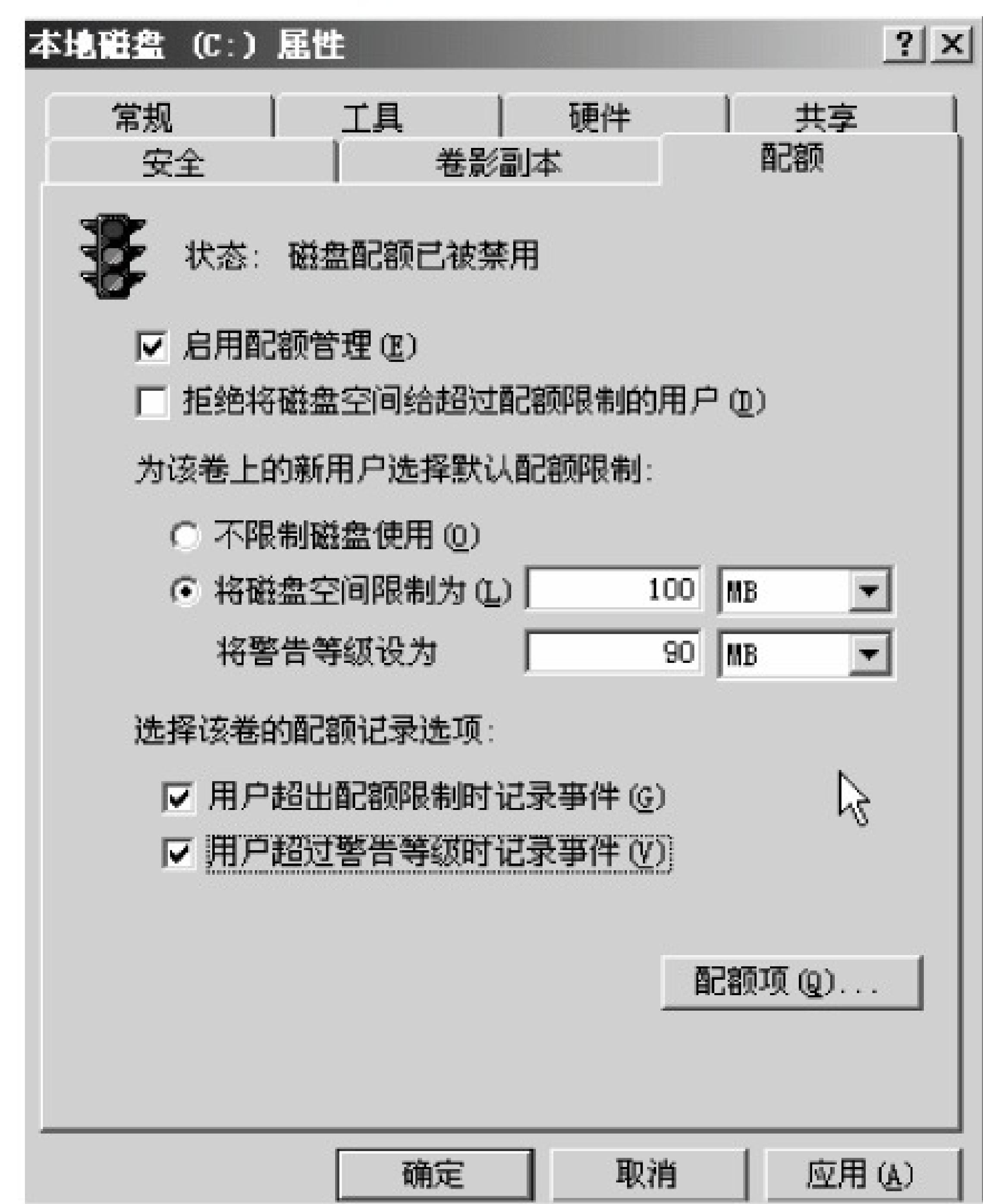


图 6-69　利用磁盘配额定制邮箱容量

② 在“配额”选项卡中，选择“启用配额管理”、“拒绝将磁盘空间给超过配额限制的用户”两个复选框。选择“将磁盘空间限制为”单选按

钮，设置配额的空间限制。在"选择该卷的配额记录选项"栏，选择是否打开"用户超出配额限制时记录事件"、"用户超过警告等级时记录事件"复选框。

③ 如果对某个用户进行特殊设置，单击"配额项"按钮，对特殊用户进行设置（如图 6-70 所示）。



图 6-70　利用配额项对个别用户进行设置

3. 建立邮件交换记录

邮件交换器资源记录是电子邮件服务器专用的，用于电子邮件应用程序发送邮件时根据收信人的地址后缀来定位邮件服务器，即根据收信人邮件地址中的 DNS 域名，向 DNS 服务器查询邮件交换器资源记录，定位要接收邮件的邮件服务器。具体设置步骤如下。

（1）执行菜单命令"开始"→"管理工具"→DNS，打开"域名系统（DNS）"对话框，建立区域如 sdcit. com 区域，并在 sdcit. com 下建立主机名 pop3. sdcit. com 和 smtp. sdcit. com，用鼠标右击 sdcit. com 域名，从弹出的快捷菜单中选择"新建邮件交换器（MX）"项。

（2）打开"新建资源记录"对话框，如图 6-71 所示，单击"浏览"按钮。

（3）在"浏览"对话框中，双击"主机名"，选择"正向查找区域"，选择 sdcit. com 项，选择 pop3 主机，如图 6-72 所示。单击"确定"按钮。

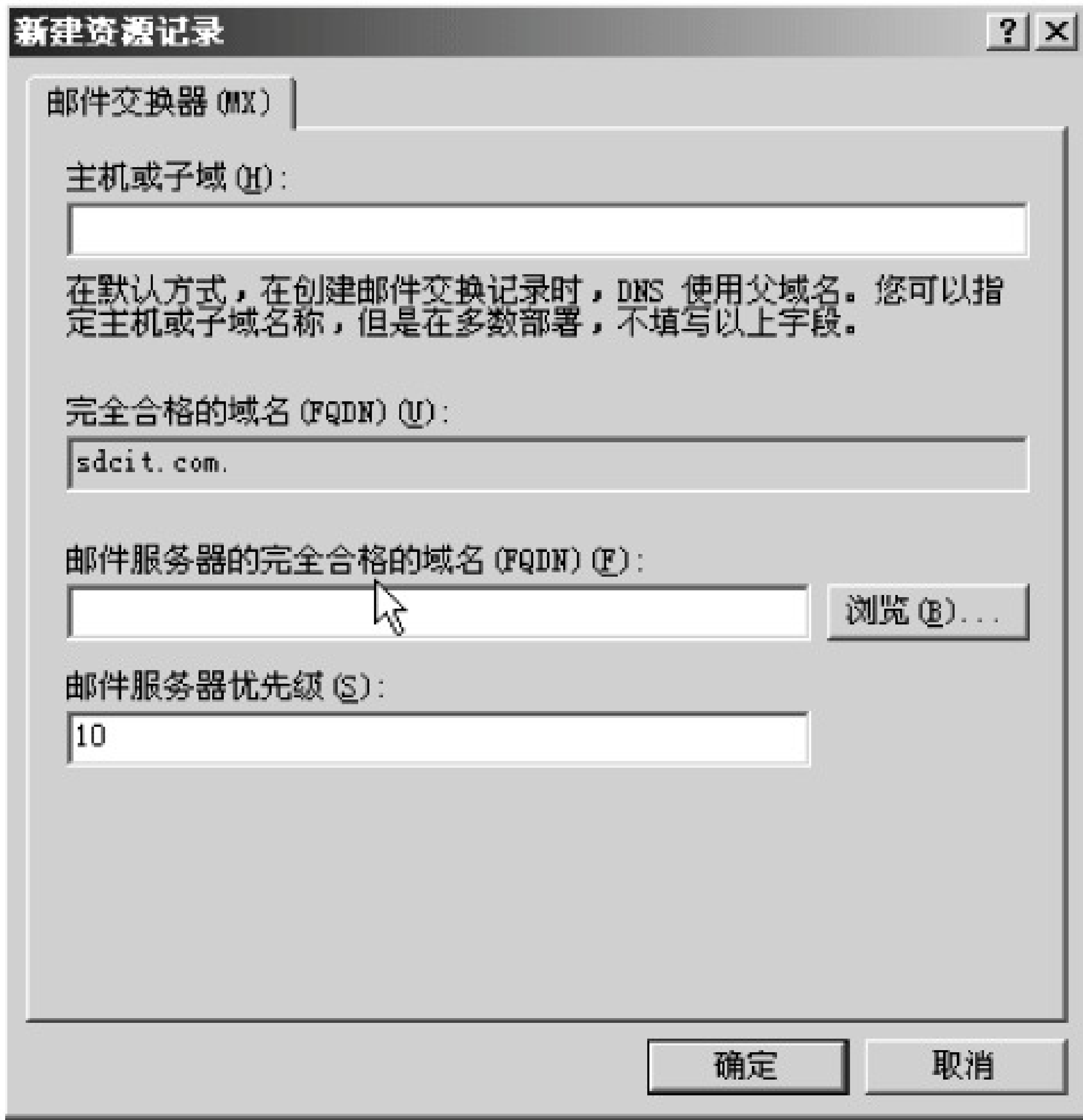


图 6-71　新建资源记录



图 6-72　浏览

（4）在返回的“新建资源记录”对话框中单击“确定”按钮。

4．SMTP 服务器的配置

SMTP 服务安装完成后，需要经过相应的设置后才能工作，其设置步骤如下。

（1）进入“Internet 信息服务（IIS）管理器”窗口，右击“默认 SMTP 虚拟服务器”选项，从快捷菜单中选择“属性”项。

（2）打开“默认 SMTP 虚拟服务器属性”对话框，在“常规”选项卡的 IP 地址栏中选择要为 SMTP 绑定的 IP 地址，单击“确定”按钮。

5．客户端配置

当 POP3 服务和 SMTP 服务安装设置完成后，就可以利用电子邮件客户端软件进行收发了。

任务完成：Windows Server 2003 系统中常用的一些服务器软件，根据所学的安装和使用步骤，发挥它们的功效。

知识拓展——WINS 服务器

在计算机网络中，客户端计算机在 Internet 协议网络中寻找其他计算机的主要方法是使用域名系统 DNS。但是，一些较早版本的 Windows 客户端仍然需要在网络通信中使用“网络基本输入/输出系统”（NetBIOS）名称，所以需要通过使用“Windows Internet 命名服务”（WINS）来注册 NetBIOS 计算机名并负责将其解析成 IP 地址。

利用 WINS 服务实现 NetBIOS 的名称解析，分为以下两个过程：

（1）客户端注册。当客户端启动时，会利用点对点的方式，直接与 WINS 服务器接触，以便将其计算机名称与 IP 地址的对照数据注册到 WINS 服务器数据库内。当 WINS 服务器接收到请求后，先核查有无重复数据，判断是否接受请求，并通知客户端。

服务器的响应如下。

① 没有响应：多次尝试后客户端自动向其他 WINS 服务器发出请求。

② 接受：若没有重复名称存在，WINS 服务器接受其注册并回应一个确定信息，包括客户端可以使用该名称的时间长度等。

③ 不接受：若该名称已被其他 WINS 客户端注册，WINS 服务器会向拥有此名称的客户端查询，若有响应则 WINS 服务器不接受新的注册请求。回应不接受信息。

（2）NETBIOS 名称解析。指把计算机的 NetBIOS 名称映射到 IP 地址的过程。必须先将 NetBIOS 名称解析成 IP 地址，然后才能将 IP 地址解析为硬件地址。解析方式如下：

① NetBIOS 名称缓存。每台运行 Windows 操作系统并使用 NetBIOS 的计算机会在内存中维护一个 NetBIOS 名称缓存。名称项在 NetBIOS 名称缓存中保存的时间相对较短（默认情况下，Windows 2000 是 10 分钟）。

② NetBIOS 名称服务器。NetBIOS 名称服务器维护了一个包含 NetBIOS 名称和 IP 地址的数据库，它会对名称解析请求进行响应。在 Windows 2000 中，WINS 服务器就是 NetBIOS 名称服务器，负责注册，响应查询。

③ NetBIOS 名称节点解析法。另一种 NetBIOS 名称解析成 IP 地址的方法称为节点法。

B-节点(广播)使用广播方式注册和解析名称。广播方式会增加网络流量的负担,路由器又不转发广播消息,因此无法跨越到另一个网络区域。

P-节点(对等)使用 NetBIOS 名称服务器来解析 NetBIOS 名称,使用点对点的方式,直接向 WINS 服务器查询对方的计算机的 IP 地址,然后由 WINS 服务器将其 IP 地址提供给计算机,不使用广播,因此可跨越到另一个网络区域。

M-节点(混合)组合了 B-节点和 P-节点,默认情况下按 B-节点工作,如果无法通过广播来解析名称,它将使用 P-节点的方法向 WINS 服务器查询对方计算机的 IP 地址。

H-节点(混合)组合了 P-节点和 B-节点,先向 WINS 服务器查询 IP 地址,如果失败,再用广播的方式查询。

B-节点方式还有一种扩充功能:当广播查询失败时可以尝试到 LMHOSTS 文件内去查找,可以解决广播无法跨越路由器的缺点。

实训 6 FTP 服务器的使用

1. 实训目的

(1) 掌握利用 Windows XP 建立 FTP 服务器的方法。

(2) 掌握 FTP 服务器的配置和管理的方法。

(3) 掌握访问 FTP 服务器的方式。

2. 实训内容

(1) 安装、配置及管理 Windows XP 服务器的 FTP 服务。

(2) 掌握访问 FTP 服务器的基本方式。

3. 实训步骤

(1) 在服务器上安装 FTP 信息服务组件,以管理员身份登录。

(2) 启动默认的 FTP 服务器。

① 从“程序”菜单中依次选择“管理工具”→“Internet 信息服务(IIS)管理器”命令,在控制台下右击“默认 FTP 站点”选项,选择“启动”命令。

② 在控制台中右击“默认 FTP 站点”选项,选择“属性”命令,进入默认 FTP 站点属性对话框,查看网络客户连接本 FTP 服务器所需要使用的 IP 地址和 TCP 端口。

(3) 配置默认 FTP 站点。

① 在某个分区下,例如 D 分区,建立文件夹 FTP,作为默认 FIP 站点的主目录。

② 在 FTP 文件夹下新建文本文档,任意写入一些内容。

③ 建立虚拟目录。

(4) 访问默认 FTP 站点。

(5) FTP 客户端程序的使用。

4. 实训要求

(1) 记录配置 FTP 服务器中的主要参数。

(2) 思考并回答：建立虚拟目录的过程及其作用是什么。

习　题　6

1. 选择题

(1) 在设备管理器中如果设备有故障或没有安装驱动程序，会在该设备前面显示一个(　　)色的问号。

A. 红　　B. 黄　　C. 蓝　　D. 黑

(2) 下面从大到小排列正确的是(　　)。

A. 对象、组织单位、域、域树　　B. 组织单位、对象、域、域树

C. 域树、域、组织单位、对象　　D. 对象、组织单位、域、域树

(3) Windows Server 2003 默认建立的用户账户中，默认被禁用的是(　　)。

A. Administrator　　B. Guest　　C. HelpAssistant　　D. Users

(4) 本地计算机 A 是域 B 的成员之一。本地用户 Max 属于 Administrators 组，当他登录域的时候，却无法执行任何系统管理功能。怎样使 Max 可以完全控制登录的计算机？(　　)

A. 删去本地用户账户 Max

B. 将 Max 的域用户账户加入到 Administrators 组

C. 将 Max 的域用户账户加入到域的 Administrators 组

D. 赋予 Max 对 C:\WINNT 目录的完全控制权限

(5) DNS 提供了一个(　　)命名方案。

A. 分级　　B. 分层　　C. 多级　　D. 多层

(6) Internet 管理结构最高层域划分中表示商业组织的是(　　)。

A. COM　　B. GOV　　C. MIL　　D. ORG

(7)(　　)表示别名的资源记录。

A. MX　　B. SOA　　C. CNAME　　D. PTR

(8) Web 主目录的访问权限不包括(　　)。

A. 读取　　B. 更改　　C. 写入　　D. 目录浏览

(9) Web 网站的默认端口为(　　)。

A. 8080　　B. 8000　　C. 80　　D. 8008

2. 填空题

(1) Windows Server 2003 有 4 个版本，分别为：________、________、________、________。

(2) 推荐 Windows Server 2003 安装在________文件系统分区。

(3) Windows Server 2003 中共享文件夹的访问权限主要有________和________，如果两者都可以，则为________。

（4）DHCP 中文名称________。

（5）FTP 站点可设置的消息有：________、________、________和________。

（6）在 Internet 信息服务管理器中，设置 FTP 站点的访问权限有________和________。

3．简答题

（1）NTFS 文件系统的权限特性是什么？

（2）动态 IP 地址方案有什么优点和缺点？

模块 7　网络管理与网络安全

任务 7.1　安全防护与病毒检测

任务描述：计算机技术和网络技术为人类带来了方便和快捷，同时也伴随着各种威胁。由于计算机网络本身有漏洞，加上黑客、病毒、木马的威胁，人们越来越关心计算机本身和网络信息的安全性问题。

7.1.1　网络安全概述

随着计算机技术和网络技术的飞速发展，网络和信息已经成为人们生活中必不可少的一部分，是关乎国计民生的重要方面。现在人们越来越关心网络信息的安全性问题。网络应用已渗透到现代社会生活的各个方面，电子商务、电子政务、电子银行等无不关注网络安全。至今，网络安全不仅成为商家关注的焦点，也是技术研究的热门领域。

由于计算机网络本身有漏洞，加上黑客、病毒、木马等严重威胁着网络安全。目前，网络安全是计算机网络的一个重要研究项目。随着网络规模越来越大，越来越复杂，网络安全的要求也越来越高。

计算机网络安全主要涉及网络信息的安全和网络系统本身的安全。计算机网络系统本身的一些硬件设施，如计算机、服务器、交换机、传输线路等，可能面临着遭到攻击和破坏，其中存储的数据信息也可能被盗用、篡改和破坏。计算机网络系统的软件漏洞，以及一些黑客、恶意程序的攻击也会增加网络安全的难度。

1. 网络安全的意义

网络技术的迅速发展的确是给社会的发展带来了巨大的方便，人们可以足不出户地完成一系列工作，如网上购物、收发电子邮件、电子商务等，现在的社会可以说是一个网络社会。但是网络给人们带来方便的同时，也带来了一系列的网络安全问题。

伴随着计算机技术与通信技术的迅速发展，网络安全的威胁和防范技术也是循环上升，只要是接入到 Internet 中都有可能遭到攻击或破坏。如果网络安全没有保障，会影响到整个网络的发展，进而影响到社会文明的进步。网络不仅是商业交易，学习办公，娱乐休闲的场所，更是国家重要的信息基础设施建设的组成。信息网络安全体系建设对现代社会的经济生活具有重要的战略意义。

2. 网络安全的概念和特征

从本质上讲，网络安全是指通过采用各种技术和管理措施，保护网络系统的硬件、软件和系统中的数据，不受偶然或恶意的原因遭到破坏、更改、泄露，使网络系统正常运行，网络服务不中断。

广义上讲，只要是涉及网络上的信息数据的可控性、完整性、可用性、保密性和不可否认性等相关技术和理论都是属于网络安全的领域。

网络安全是一个不断变化、快速更新的领域，更是一个系统工程。网络系统安全的建设是一个长期的过程。网络安全技术包括身份认证、访问控制、数据保密和完整性、网络交易不可抵赖，以及可用性和可靠性等。涉及 OSI 的 7 个层次，这是个多方面、多层次、立体的系统问题。

计算机网络的发展使信息的应用日益广泛和深入，但是信息在存储传递过程中会被非法地窃取、泄露、截获、篡改，导致不可估量的损失。所以要保证网络的安全性，要具备以下特征：

（1）完整性，网络系统中存储和传递的数据信息不被非法操作，即不被修改、丢失和替换。

（2）保密性，保证信息在系统中不泄露给非法用户或者非授权用户等不相关的人员，仅供授权用户使用。

（3）可控性，对危害信息的监控审计工作。

（4）可用性，保证软件和数据完整的同时，正常的信息资源服务功能和操作。

（5）不可否认性，对出现的安全问题提供调查的依据和手段。使用审计、监控和防止抵赖等机制，使破坏者、攻击者、抵赖者不能否认自己的行为。

随着计算机安全问题的凸显，美国国防部将计算机的安全等级划分为 4 个大类——D、C、B、A，细分为 7 个小类——D、C1、C2、B1、B2、B3 和 A1。

- D 类：最低保护，没有安全功能。
- C1 类：选择性安全保护。设置一个防止破坏的区域，其中包含安全功能。但不能控制用户的访问级别。
- C2 类：受控的访问控制。该级别允许或拒绝任何用户访问单个文件。具有审计跟踪能力。对某一目录有访问权限，对其内的所有程序和数据有访问权限。
- B1 类：有标签的安全保护。每个用户都有一个许可级别，文件所有者也不能随意改变文件许可权限。
- B2 类：结构化安全保护。系统的设计和实现要实现彻底的测试和审查。须对所有目标和实体实施访问控制。
- B3 类：安全域机制。系统的安全功能足够小。要求用户通过一条可信任的途径连接到系统上。
- A1 类：核实保护。包含一个严格设计、控制和验证过程。

我国在 2001 年实施的《计算机系统安全保护等级划分准则》，将信息安全分为 5 个等级。

自主保护级：相当于 C1 级。

系统设计保护级：相当于 C2 级。

安全标记保护级：相当于 B1 级，属于强制保护。

结构化保护级：相当于 B2 级。

访问验证保护级：相当于 B3～A1 级。

实际应用中，主要考核的安全指标有身份认证、访问控制、数据完整性、安全审计、信道分析等。

7.1.2 网络安全的威胁与对策

计算机网络上存在的威胁主要分为主动攻击和被动攻击两大类,共有以下4种:

- 篡改:故意修改存储或传递的数据内容。
- 截获:非法地窃取他人的数据内容。
- 拒绝服务:阻止或中断通信的正常服务,使双方的信息传递不能正常进行。
- 伪装:冒名顶替,一般来说,伪装的威胁中伴随着其他的威胁。

其中除了截获属于被动攻击外,其他的都属于主动攻击。

网络安全威胁从形式上分主要有:非授权访问(如假冒、身份攻击、非法用户进入系统等)、泄露信息(黑客攻击等)、破坏信息、计算机病毒、木马、拒绝服务等。

1. 计算机病毒的检测和查杀

(1) 计算机病毒的定义

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义,病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

计算机病毒是人为编写的一个程序,一组可执行代码。其特征就像生物病毒一样,有强大的自身复制能力。它们能把自身附着在各种类型的文件上,感染这些文件。当感染文件被复制时计算机病毒同样会跟着复制文件移动,从一个用户传送到另一个用户,它们就随同文件一起蔓延开来,而又常常难以根除。

(2) 计算机病毒的特点

计算机病毒具有以下几个特点。

① 传染性。传染性是病毒的基本特征。计算机病毒不但本身具有破坏性,更有害的是具有传染性。病毒程序通过修改磁盘扇区信息或文件内容,把自身嵌入到其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。

② 潜伏性。病毒侵入后,一般不立刻发作,需要等一段时间,条件成熟后才起作用。有些病毒像定时炸弹一样,发作时间是预先设计好的。比如黑色星期五病毒,潜伏期间不容易被发现,而到了预定时间就会发作,对系统进行破坏。

③ 隐蔽性。病毒程序大多夹在正常程序之中,很难被发现。有的可以通过病毒软件检查出来,有的根本就查不出来,这类病毒处理起来通常很困难。

④ 破坏性。计算机中毒后,可能会导致正常的程序无法运行,计算机内的文件被删除或计算机本身受到不同程度的破坏。其表现为占用大量的CPU时间和内存开销,从而造成进程堵塞;对数据或文件进行破坏;打乱屏幕的显示等。

除了上述特点外,病毒还具有触发性、衍生性、寄生性、持久性等。这里就不详细讲述了。

(3) 计算机病毒的危害

计算机病毒破坏系统的数据,甚至导致系统瘫痪。主要表现在如下几个方面:破坏磁盘文件分配表;删除磁盘上的文件;修改或破坏文件的数据;产生垃圾文件;破坏硬盘的主扇区;破坏主板上的BIOS内容;破坏网络中的资源;占用CPU运行时间,使运行效率降低;破坏屏幕的正常显示,干扰用户的操作;破坏键盘的输入程序,使用户的正

常输入出现错误；破坏系统设置或对系统信息进行加密，使用户工作紊乱。

（4）计算机病毒的分类

按照病毒的传染途径可以分为引导型病毒、文件型病毒和混合型病毒。

引导型病毒：感染对象是计算机存储介质的引导扇区，取代正常的引导记录，将正常的引导记录隐藏在其他存储空间中。

文件型病毒：感染可执行文件。在每次激活时，感染文件把自身复制到其他可执行的文件中，并能在内存中保存很长的时间。当用户调用感染了病毒的可执行文件时，病毒首先被运行，然后感染其他文件。该病毒的特点是依附于正常文件，成为程序文件的一个外壳或部件。

混合型病毒：兼有引导型病毒和文件型病毒的特点。

（5）计算机病毒的防范方法

预防计算机病毒的保护措施主要有：一是在管理上的措施，尽早发现疫情，及时修复系统；二是尽可能及时修补计算机上的系统漏洞；三是使用功能强大的、更加完善的、具有超强防御能力的杀毒软件。具体操作包括：

① 正确配置 Windows 操作系统，正确配置可以使 Windows 系统免遭病毒的侵害。

② 经常对系统进行升级并下载最新补丁。

③ 正确配置网络。

首先，将网络文件和打印机共享去掉。

操作方法：右击“网上邻居”图标，选择“属性”选项，右击窗口中的“本地连接”，选择“属性”选项，出现如图 7-1 所示的对话框，取消“Microsoft 网络的文件和打印机共享”复选框的选择。

其次，将不需要的端口禁用。

操作方法：在图 7-1 中，选择“Internet 协议(TCP/IP)”选项，单击“属性”按钮，单击“高级”按钮，打开“选项”选项卡，双击“TCP/IP 筛选”选项，选择“启用 TCP/IP 筛选(所有适配器)”复选框，并选择系统只对外开放的端口即可，如图 7-2 所示。

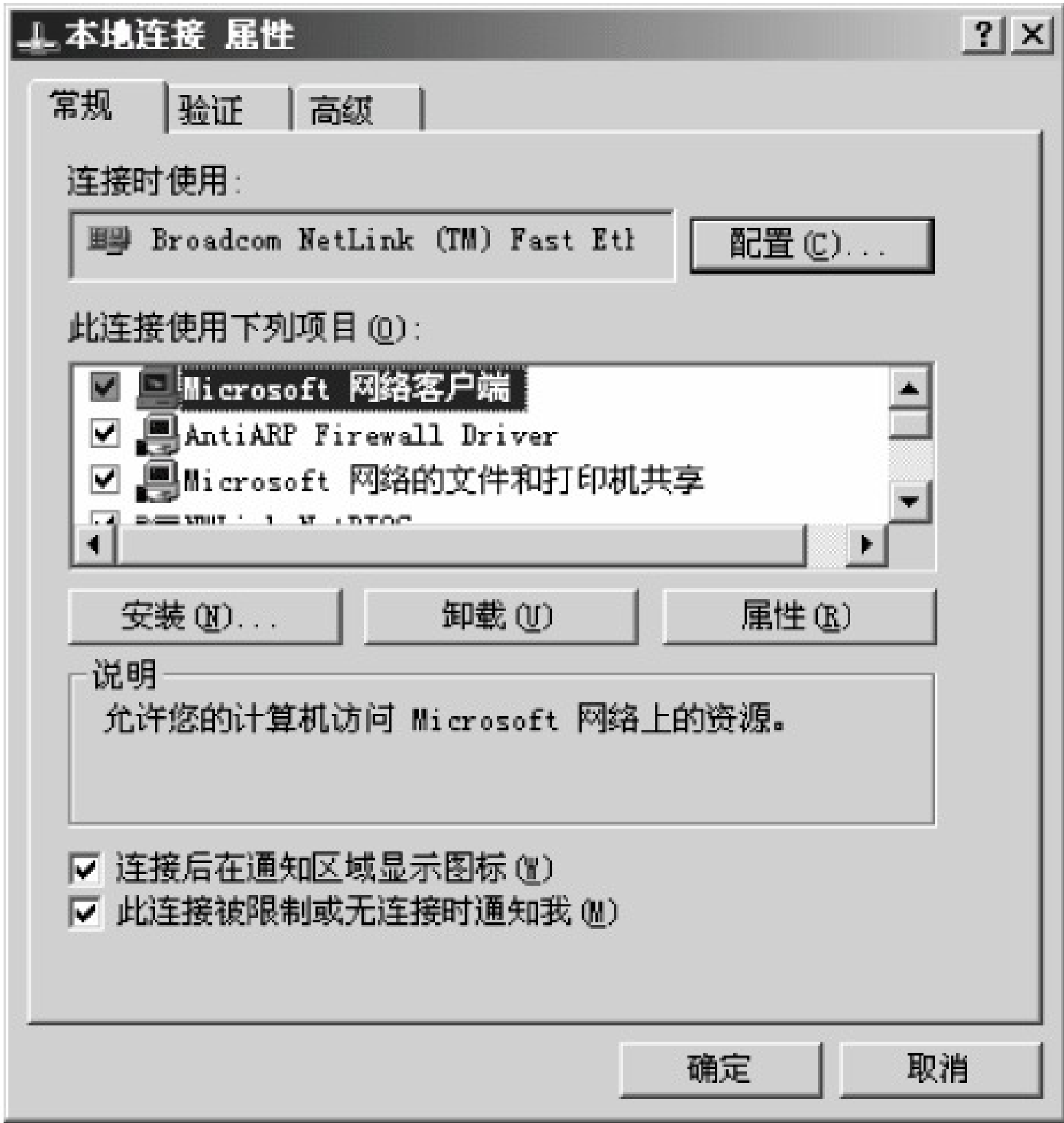


图 7-1　本地连接属性

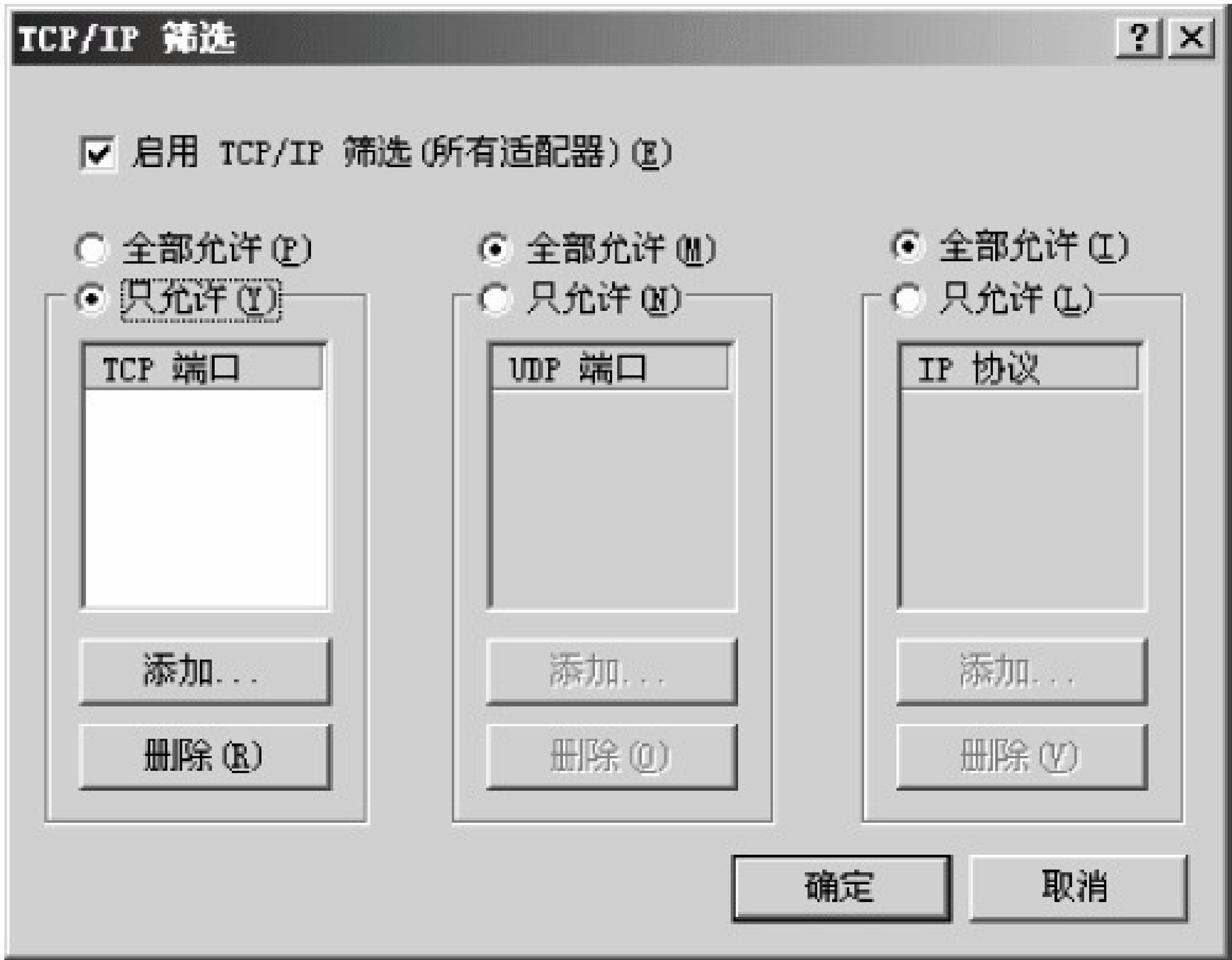


图 7-2　启用 TCP/IP 筛选机制

最后，正确配置服务，将系统不必要的服务关闭。

具体操作为：在“控制面板”窗口中双击“管理工具”图标，选择“服务”选项，将不需要的服务设置为禁用。

④ 利用 Windows 系统自带的工具。

一是利用注册表工具。

在运行窗口中，执行注册表编辑命令 regedit，打开注册表编辑窗口，检查病毒。如果在“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run”下发现有一些奇怪的键值，就说明系统可能感染了病毒。因为在该主键下，所有注册的程序都会在 Windows 启动时自动运行，而病毒也会使自己的启动自动运行，从而获取系统的控制权。

二是利用 Msinfo32. exe 命令。

Msinfo32. exe 命令提供了一个系统信息查看工具。如图 7-3 所示，通过其中的软件环境查看系统的运行情况，在右边的窗口中可以查看有没有可疑的程序。



图 7-3　系统信息

⑤ 安装防病毒软件。

在服务器上应安装网络防病毒软件，在工作站上应安装单机环境下的反病毒软件（如金山毒霸）。并及时升级这些软件的病毒库，确保其能查杀最新的病毒。

金山毒霸是常用的反病毒软件之一，使用它可以完成病毒的监控、防御，能够主动进行系统漏洞的修补，主动实时升级。程序界面如图 7-4 所示。

金山毒霸提供了日志查看器、创建应急 U 盘、病毒隔离系统、可疑文件扫描、进程管理器、垃圾文件清理、文件粉碎器等工具。通过综合设置可以完成预设防御措施，如图 7-5 所示。

虽然病毒软件本身都有自动查毒功能。但用户在利用 U 盘、网络等传递数据时应注意病毒的清查。



图 7-4　金山毒霸主程序

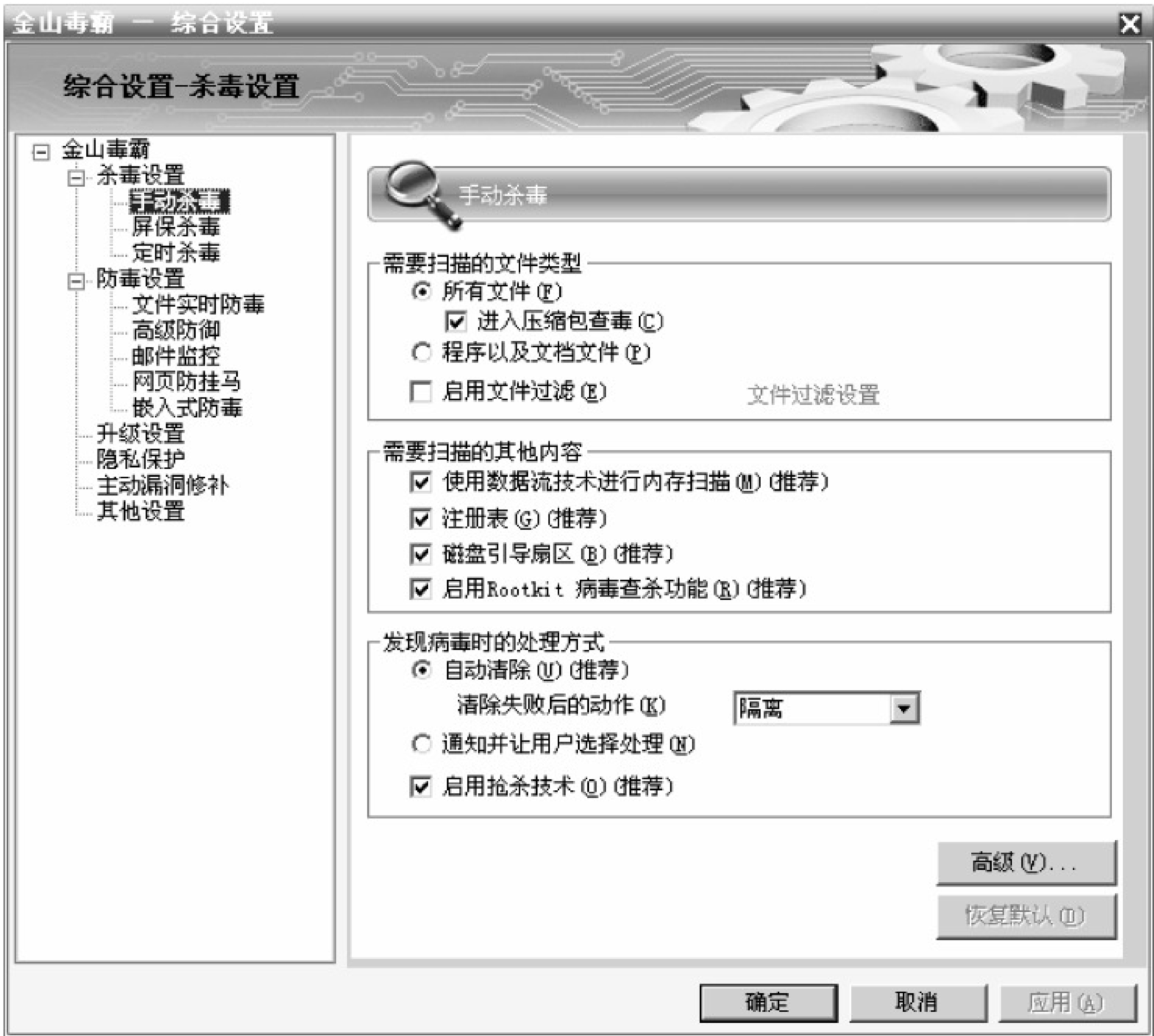


图 7-5　杀毒设置

⑥ 对下载文件要做病毒检查处理。

下载的音乐、软件等文件在应用之前要做病毒检查处理。

⑦ 电子邮件病毒的防范。

将携带电子邮件病毒的信件删除，就可以清除电子邮件病毒，但大多数电子邮件病毒

在被接收到客户端时就可能开始发作，基本上没有潜伏期，所有一般常用的预防方法有：

- 不要轻易执行附件中的 EXE 和 COM 等可执行文件。
- 不要轻易打开附件中的文档文件。应先保存到磁盘上，用杀毒软件检查无毒后再打开使用。
- 删除文件扩展名很奇怪的附件，如 *.VBS、*.SHS 等的附件。
- 使用 Outlook Express 收发电子邮件，应当进行一些必要的设置。如在菜单命令“工具”→“选项”的“安全”选项卡下的设置：在“其他”选项卡中单击“高级选项”按钮，单击“加载项管理器”，取消“服务器脚本运行”选项；在“阅读”选项卡中，取消“在预览窗各种自动显示新闻邮件”和“自动显示新闻邮件中的图片附件”选项。这样可以防止有些电子邮件病毒利用 Outlook Express 的默认设置自动运行，破坏系统。

对于自己往外传送的附件，应确定无毒后，才可发送。

(6) 常见病毒简介

① CIH 病毒

该病毒基本上通过网络或盗版光盘传播。在执行了被感染的文件后，CIH 病毒会感染与被执行文件接触到的其他程序。它将自身代码拆分为多个片段，然后依靠移动、可执行形式将这些片段放到 Windows 文件未使用的磁盘空间里。它发作时会破坏硬盘的引导区和分区表，而且破坏 Flash BIOS 芯片中的系统程序，导致主板损坏。

判断是否感染 CIH 病毒。先运行一个程序，如 Word；然后执行“开始/搜索—所有文件和文件夹”，输入内容如图 7-6 所示。若查找到，就有可能感染了 CIH 病毒。

防范设置方法。BIOS 设置中将“BIOS 写保护”项设置为 Enable；将 Flash ROM 跳线设置为不可改写（注意：一些芯片的读写和改写电压一样，就不能用这种设置）；若不升级 BIOS，可以将 Flash 芯片的改写电压的管脚去掉；BIOS 设置中的 Boot Sector Virus Protection 设置为 Enable，将对硬盘的改写在 BIOS 的监控之下。

清除病毒，利用杀毒软件完成。

② 宏病毒

病毒代码以“宏”的形式潜伏在 Office 文件中，主要感染 Word 和 Excel 等文件。病毒通过文件的打开或关闭来获取控制权，然后进一步获取一个或多个系统事件，并通过这些事件调用完成对文件的感染。宏病毒的防范和清除方法有：

禁止使用自动执行的宏，Word 2003 中的设置方法是：单击“工具”菜单，选择“宏”→“安全性”，打开“安全性”设置对话框，如图 7-7 所示。

检查宏，看是否有可疑的宏，如果有则删除。

备份通用模板 Normal.dot，若怀疑有宏病毒，则用备份替换当前的 normal.dot 模板。

设置“如果改写模板要提示”：执行菜单命令“工具”→“选项”，在“保存”选项卡中，选择“提示保存 Normal 模板”。当提示保存会修改公用模板，说明已感染了宏病毒，应选择否，退出，再用杀毒软件杀毒即可。

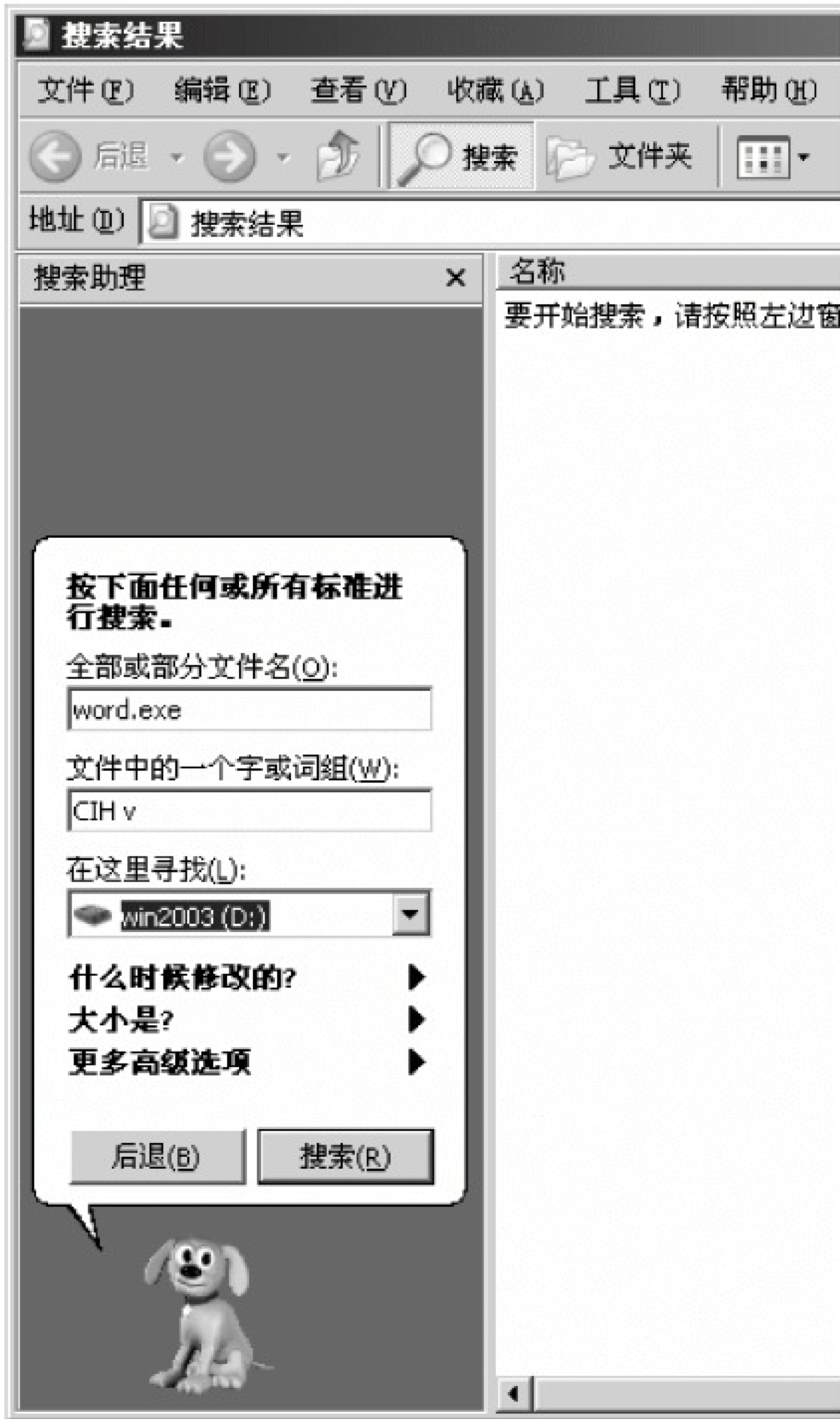


图 7-6　搜索结果

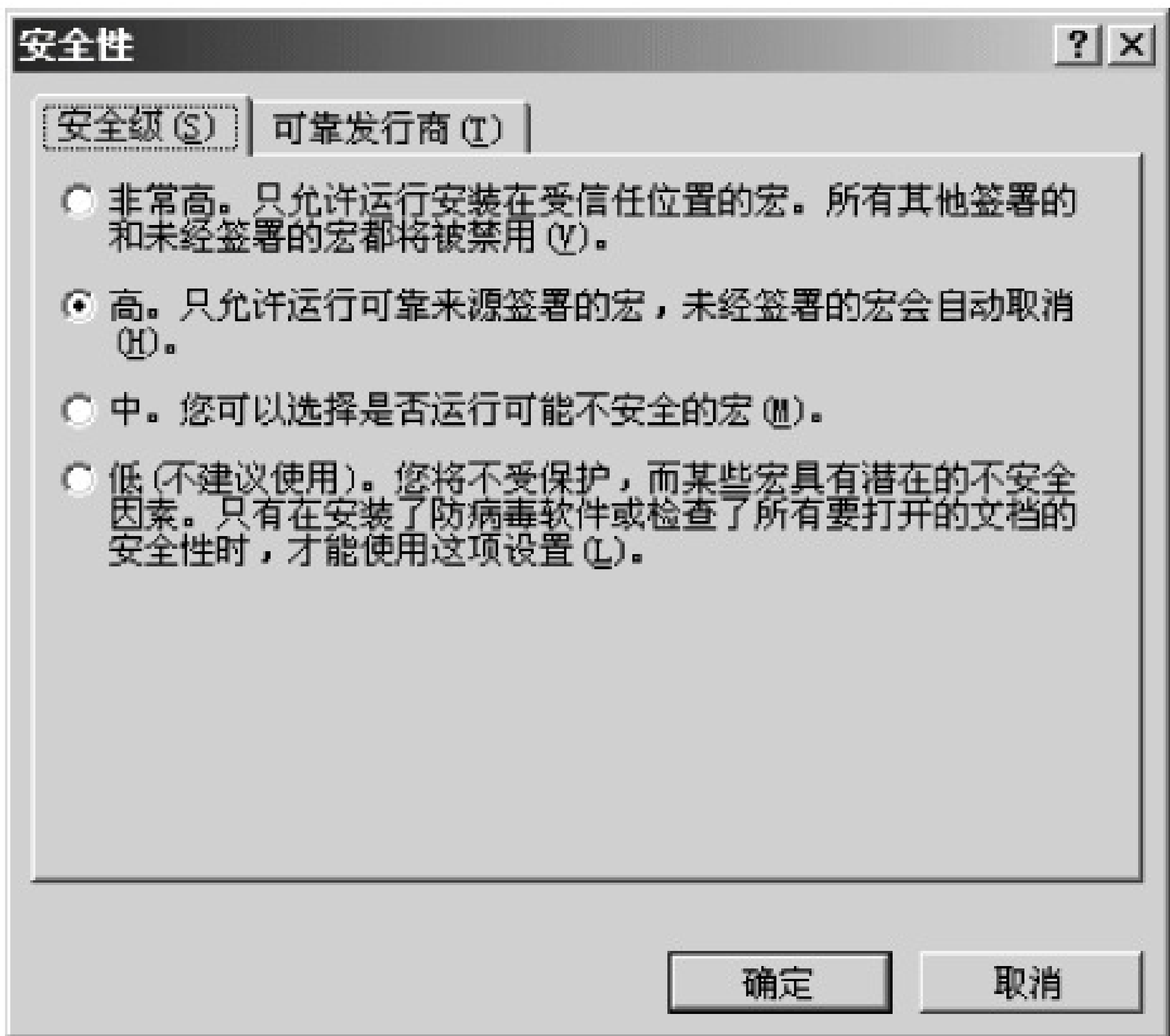


图 7-7　安全性

③ 冲击波病毒(WORM_msblast.A)

冲击波病毒利用 Windows 操作系统的漏洞实施攻击。受到冲击波病毒攻击后的主要特征有反复重新启动计算机、Windows 界面的某些功能无法正常使用、Office 等文件无法正常使用、网络速度明显变慢、IE 浏览器无法打开链接等。

冲击波病毒的感染过程主要表现为：病毒将自身复制到 Windows 目录下，名字为“msblast.exe”；病毒运行时在系统中建立一个名为“BILLY”的互斥量，目的是使病毒自身不重复进入内存，只保证内存中有一份病毒体，避免用户发现；运行时会有一个“msblast.exe”进程。

病毒会修改注册表，在 Run 下添加键值“windows auto update”为“msblast.exe”，便于机器启动，病毒就运行；病毒隔 20 秒检测一次网络状态，当网络可用时，在 UDP69 端口建立一个 TFTP 服务器，并启动一个攻击传播线程，随机生成攻击地址攻击，一般就近攻击；病毒扫描到计算机后，向目标计算机的 TCP135 端口发送攻击数据；病毒攻击成功后，会监听目标计算机的 TCP4444 端口作为“后门”，并绑定“cmd.exe”文件，蠕虫会连到该端口，发送 tftp 命令，回连到发起攻击的主机，同时将“msblast.exe”传送到目标计算机上运行；即使没有攻击成功，也会造成系统的 RPC 服务崩溃。例如微软的更新站点曾经受到攻击，无法为用户提供服务。

冲击波病毒的防范方法如下：断开与网络的所有连接；在任务管理器中，终止“msblast.exe”进程的运行；在注册表中删除病毒对应的键值；关闭相应的端口(防火墙

配置)等。

④ 震荡波病毒

该病毒利用 Windows 平台的“安全认证子系统”的 Lsass. exe 漏洞进行传播,攻击远程计算机的 445 端口,感染后的系统将开启 128 个线程去攻击其他网上的用户,造成机器运行缓慢、网络堵塞,并导致计算机不断地重新启动。该病毒会在网络上自动搜索系统有漏洞的计算机,并直接引导这些计算机下载病毒文件并执行,整个传播和发作过程不需要人为干预。该病毒在 RUN 下建立的键值是“avserve. exe=%windows%\avserve. exe”。对有漏洞的计算机,打开 TCP 的 5554 端口传播病毒文件。

病毒特征:系统感染病毒后,开启多个线程,占用大量的系统资源,使 CPU 占用率达到 100%,系统运行缓慢;产生一个“avserve. exe”进程,在系统安装目录下有一个“avserve. exe”程序;注册表在 RUN 下建立的键值是“avserve. exe”为“%windows%\avserve. exe”。

病毒的清除。断开网络;查找名为“avserve. exe”和“*_up. exe”的文件,删除;运行注册表编辑器,删除对应的键值;关闭 TCP 的 5554 端口,以阻止 SASSER 蠕虫通过 TCP 进行文件传输;运行杀毒软件杀毒。

2. 黑客攻击及其防范

(1) 黑客攻击

黑客(Hacker)是热衷于计算机程序的设计者,对任何计算机系统都很有兴趣的人,他们的行为一般没有恶意。另一类称为骇客,他们的行为是具有恶意的,指那些强行闯入别人的计算机系统或者以某种恶意的目的干扰远端系统,非法获得访问权,破坏数据,拒绝服务等。

黑客入侵的常用手段是获得超级用户口令。先是通过运行的应用程序找到可以利用的漏洞,在此基础上获得用户的权限,然后再去达到目的。

(2) 黑客攻击的工具

黑客进行网络攻击常用的手段有获取口令(通过网络监听获取口令,或在知道用户的账号的前提下,利用一些专门的软件强行破解用户口令,或在获得一个服务器上的用户口令文件后用破解程序破解用户口令)、放置木马程序、利用电子邮件攻击、拒绝服务攻击、IP 地址欺骗等。

① 木马

木马(Trojan)这个名字来源于古希腊传说,特洛伊木马是指一种计算机程序,它驻留在计算机里,当计算机启动时自动运行木马程序,且木马的服务一旦运行并被控制端连接,其控制端将享有服务端的大部分操作权限,例如给计算机增加口令、浏览、移动、复制、删除文件、修改注册表、更改计算机配置等。

木马的最主要特征是隐蔽性和功能特殊性。木马软件在运行时,采用各种手段隐藏自己,通过修改注册表和“. ini”文件以便在下次启动后加载程序。特殊功能性是指除了具有普通文件的操作功能外,还具有设置口令、记录键盘、修改注册表、更改配置等功能。

木马系统的组成主要有硬件部分、软件部分和具体连接部分。

硬件部分是建立木马连接所必需的硬件实体。具体组成是：控制端是在服务端进行远程控制的一方；服务端是被控制端远程控制的一方；Internet 是控制端对服务端进行远程控制和数据传输的网络载体。

软件部分是实现远程控制所必需的软件程序。控制端程序是在控制端用以远程控制服务端的程序；木马程序是潜入服务端内部，获取其操作权限的程序；木马配置程序是设置木马程序的端口号、触发条件、木马名称等，使其在服务端藏得更隐蔽的程序。

具体连接部分是通过网络在服务端和控制端之间建立一条木马通道。控制端和服务端的网络地址、控制端和木马端口号等。

预防木马的危害，主要采取以下措施：

第一，安装正版的杀毒软件和个人防火墙，及时升级，并且设置好安全等级，防止未知程序向外传送数据。

第二，尽量使用安全性比较好的浏览器工具和电子邮件客户端程序。

第三，防止恶意网站在自己计算机上安装不明软件和浏览器插件，以免被木马趁机侵入。

常见国产木马的清除方法如下。

- 冰河木马

冰河创造了最多人使用、最多人被植入的奇迹，可以说是最著名的木马了。现在网上有许多冰河的变种程序。

冰河的服务器端程序为“G-server. exe”，客户端程序为“G-client. exe”，默认端口是 7626，一旦运行“G-server. exe”，则在系统目录下生成“Kernel32. exe”和“Sysexplr. exe”并删除自身。“Kernel32. exe”在系统启动时自动加载运行，“Sysexplr. exe”和“TXT”文件连接，即使删除了“Kernel32. exe”，但只要打开“TXT”文件，“Sysexplr. exe”就会被激活，它将再次生成“Kernel32. exe”。

清除冰河的步骤如下。

删除“C：\Windows\system”下的“Kernel32. exe”和“Sysexplr. exe”文件。

将注册表“HKEY_LOCAL_MACHINE\software\microsoft\windows\Current Version\Run”下的键值“C：\windows\system\Kernel32. exe”的键值删除。

将“HKEY_LOCAL_MACHINE\software\microsoft\windows\Current Version\Runservices”下的“C：\windows\system\Kernel32. exe”键值删除。

修改注册表“HKEY_CLASSES_ROOT\txtfile\shell\open\command”下的默认值，由个人密码后的“C：\windows\system\Sysexplr. exe %1”改为正常值“C：\windows\notepad. exe %1”，恢复 TXT 文件的关联功能。

- 广外女生

广外女生是一种远程监控工具，破坏性很大，可远程上传、下载、删除文件、修改注册表等。其服务器端被执行后，会自动检查进程中是否含有“金山毒霸”、“防火墙”、“实时监控”等防护，若发现就将该进程终止，使防护失去作用。该程序运行后在系统目录下生成自己的复制文件“diagcfg. exe”，并关联 EXE 文件的打开方式，若删除了该文件，所有的 EXE 文件将无法打开。

清除步骤如下：

进入 DOS 模式，将 System 目录下的“diacfg. exe”删除。

将 Windows 目录下的注册表编辑器“regedit. exe”改名为“regedit. com”；

返回 Windows 模式下，运行“regedit. com”文件。

将“HKEY_CLASSES_ROOT\exefile\shell\open\command”的默认值改为“‘%1’%*”；

删除“HKEY_LOCAL_MACHINE \ software \ microsoft \ windows \ Current Version \ Runservices”下名称为“Diagnostic Configuration”的键值。

关闭注册表编辑器，回到 Windows 目录，将“Regedit. com”改为“regedit. exe”。

- 网络精灵

英文名为 Netspy，默认连接端口为 7306。该系统具有注册表编辑功能和浏览器监控功能，客户端可以不用 Net Monitor，通过浏览器可以进行远程监控。执行后会在系统目录下生成“netspy. exe”文件，同时在 Run 下建立键值“C:\windows\sysytem\Netspy. exe”。

清除方法如下：

启动机器，出现“Staring Windows”时，按 F5 键进入命令行状态，在“C:\Windows\system\”目录下输入命令“del netspy. exe”，将其删除；然后进入注册表删除 Run 下的键值。

- 黑客 2001

默认连接端口号为 2001，它具有杀除进程功能，即控制端可以随意终止被控端的进程。黑客 2001 服务器端被执行后，在系统目录下生成两个文件：“S_Server. exe”和“Windows. exe”。“S_Server. exe”是服务器端的直接复制，图标显示是文件夹；“Windows. exe”用未定义类型的图标显示，“Windows. exe”文件使机器开机时立刻运行，并打开连接端口 2001；“S-server. exe”和 TXT 文件关联。删除“windows. exe”文件不能彻底清除木马，因为当任何 TXT 文件运行时，隐蔽的“S_server. exe”被激活，它再次生成“windows. exe”文件。

清除步骤如下。

进入注册表编辑，将“HKEY_CLASSES_ROOT\txtfile\shell\open\command”的默认键值由“S_server. exe %1”改为“c:windows\notepad. exe %1”。

将 HKEY_LOCAL_MACHINE\software\classes\txtfile\shell\open\command 下的默认键值由“S_server. exe %1”改为“c:windows\notepad. exe %1”。

将“HKEY_LOCAL_MACHINE\ software \ microsoft \ windows \ currentversion \ runservices ”下的键值“windows”删除。

将系统目录下的两个文件删除(删除时先终止进程，然后删除)。

- 火凤凰 WAY2. 4

默认连接端口为 8011，它对受控端注册表的操作同本地操作一样。WAY2. 4 服务器端被运行后，在系统目录下生成“msgsvc. exe”文件，图标是文本文件，在注册表 Run 下的建立串值“msgtask”，其键值为“C:\windows\system\msgsvc. exe”。

对于该木马清除，先删除注册表的键值，再终止其进程，然后删除即可。

- 初恋情人

默认连接端口为 8311。自启动程序为“C:\WINDOWS\TEMP\Aboutagirl. exe”，

与 TXT 文件关联的文件是系统目录下的“girl. exe”。该木马故意设下陷阱，将服务器和客户端名字交换。清除步骤如下。

删除“C：\WINDOWS\TEMP\Aboutagirl. exe”文件。

将 HKEY_LOCAL_MACHINE\software\classes\txtfile\shell\open\command 下的默认键值由“girl. exe %1”改为“c：windows\notepad. exe %1”。

将 HKEY_LOCAL_MACHINE\software\classes\txtfile\shell\open\command 下的默认键值由“girl. exe %1”改为“c：windows\notepad. exe %1”。

- 网络神偷 nethief

第一个“反弹端口型”木马，服务器端（被控制端）使用主动端口，客户端（控制端）使用被动端口，当要建立连接时，由客户端通过 FTP 主页空间告诉服务器端，并进入监听状态；服务器端收到通知后，就会开始连接客户端。客户端的一般端口在“80”，不易被察觉。清除步骤如下：将 Run 下的键值“internet”（值为“internet. exe/s”）删除；删除自启动文件系统目录下的“internet. exe”程序。

- 网络公牛

默认连接端口为 23444，服务器端程序“newserver. exe”运行后会自动脱壳呈“checkdll. exe”状态，位于系统目录下，开机自动运行。运行后自动捆绑 notepad. exe，write. exe，regedit. exe，winmine. exe，winhelp. exe 等文件。并且还能捆绑在开机时自动运行的第三方软件，如播放器等；并且修改了注册表。

网络公牛没有采用文件关联功能，采用的是文件捆绑功能，易发现。

清除方法如下：删除自启动程序“checkdll. exe”；将在注册表建立的键值全部删除；检查它可以捆绑的文件，发现长度发生了变化，就删除，然后用正确的替换，第三方软件删除后重新安装。

② 拒绝服务攻击 DoS

拒绝服务是一种很简单且很有效的方式，目的是使用户请求的服务停止，破坏服务器系统的正常运行。拒绝服务的方式有很多种，常见的就是利用合理的请求占据过多的服务资源，让其他的合法请求无法得到服务。

最常用的 DoS 攻击方法如下。

- SYS flood：利用 TCP/IP 三次握手，伪造许多虚假的 IP 地址的 SYS 包，被攻击的服务器向虚假 IP 地址发送确认，得不到回应，占满空间，造成服务器拒绝的服务。
- PING 攻击：向目标端口发送超大尺寸的 ICMP 包实现。
- land 攻击：利用向目标计算机发送大量的源地址和目标地址相同的数据包，造成占用大量系统资源，从而使网络功能瘫痪。
- Smurf 攻击：使用目标主机的 IP 地址向广播设备发送请求，其他机器回应。
- 电子邮件炸弹：不断地向同一地址发送电子邮件，耗尽接收者网络的带宽。

解决的办法有：一是尽可能地修复存在的问题和系统的缺陷；二是识别和禁止使用拒绝服务的机器访问。

③电子邮件攻击

电子邮件攻击主要表现为两种方式：电子邮件欺骗和破坏、邮件炸弹。

电子邮件欺骗和破坏：假冒系统管理员，给用户发送邮件要求用户修改口令或在邮件中加载病毒或木马。针对这种威胁，建议重要信息采取数字加密认证方式发送；在局域网环境中，不要使用POP3和SMTP收发邮件。

邮件炸弹：用伪造的IP地址和电子邮件地址向同一信箱发送大量垃圾邮件。

电子邮件攻击防范：管理好自己的邮件地址，采用过滤功能，慎用自动回信功能，采用专用工具清除垃圾邮件。

7.1.3 网络安全技术

计算机网络安全包括主机上的信息存储安全和网络上的传输安全。目前常用的技术手段有加密技术、防火墙技术、身份认证技术、综合利用技术等。

1. 加密技术

在网络中进行相互通信的数据，受到的威胁主要是被非法地窃取。加密技术是防止数据被窃取导致泄密的常用方法。通常采用一定的算法对原文进行加密，然后将密文传送到目的段，即使中间被截获，也很难破解里面的内容。

密码技术结合数学、计算机科学等多种学科于一身。它不仅用于数据加密，而且还广泛用于数字签名、身份验证、系统安全等。

根据密钥类型不同可以将现代密码技术分为两类：对称加密算法（私钥密码体系）和非对称加密算法（公钥密码体系）。

对称加密算法中，数据加密和解密的密钥是采用了同一个，所以这种算法的安全性就由密钥决定。其优点是加密和解密速度快，加密强度高，算法公开；缺点是实现密钥的私密分发困难，并且在大量使用的情况下，管理密钥困难，无法完成身份认证，不便于应用在网络开放的环境中。目前最著名的对称加密算法有数据加密标准DES和欧洲数据加密标准IDEA等。

非对称加密算法中，加密和解密的密钥是不相同的，而且用加密密钥的加密数据只有采用相应的解密密钥才能解开。另外从加密密钥中来求解密密钥十分困难。在实际应用中，通常是将密钥中的加密密钥公开，而私密保留。利用公钥体系可以方便地实现加密和解密，对用户的身份进行认证，方便了实现对信息传送双方的身份的鉴别和认证。在实际应用中通常将公钥密码体系和数字签名算法结合使用，在保证数据传输完整性的同时完成对用户的身份认证。

2. 防火墙技术

防火墙是目前广泛应用的网络安全技术，是指建立在两个网络的边界上的，实现安全策略和网络通信监控，可以强制执行对内部网和外部网的访问控制的系统或系统组。通过建立一整套规则和策略来监测、限制、更改跨越防火墙的数据流，达到保护内部网络的目的。

一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近你的防御设施；三是限定用户访问特殊站点；四是为监视Internet安全提供方便。

防火墙系统不是一个单独的计算机程序或设备。防火墙系统是一种网络安全部件，是由软件、硬件或者是两者的结合组成。实现防火墙的主要技术有：数据包过滤，应用网

关和代理服务器等。

(1) 包过滤技术

包过滤(Packet Filtering)技术是指按照一定的策略对被保护网络和外部网络之间的数据包进行过滤,即在网络层对数据包进行选择,选择的依据是系统内设置的过滤参数。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素,或它们的组合来确定是否允许该数据包通过。工作在网络层和传输层。

包过滤技术作为防火墙的应用有三类:一是路由设备在完成路由选择和数据转发之外,同时进行包过滤,这是目前较常用的方式,也是比较容易实现的方式;二是在工作站上使用软件进行包过滤,这种方式价格较贵;三是在一种称为屏蔽路由器的路由设备上启动包过滤功能。

(2) 应用网关技术

应用网关(Application Gateway)技术是建立在网络应用层上的协议过滤,它针对特别的网络应用服务协议即数据过滤协议,并且能够对数据包分析并形成相关的报告。应用网关对某些易于登录和控制所有输出输入的通信环境给予严格的控制,以防止有价值的程序和数据被窃取。它的另一个功能是对通过的信息进行记录,如在什么时间用户做了什么事情。在实际工作中,应用网关一般由专用工作站系统来完成。

应用网关和包过滤防火墙有一个共同的特征,就是紧紧依靠特定的逻辑判定是否允许数据包通过,一旦符合条件,就允许计算机系统与外部建立起联系。使得内部防火墙的结构和设置状态很容易被外部所了解,使非法的访问和攻击容易得逞。

(3) 代理服务技术

代理服务(Proxy Service)也称 TCP 通道(Circuit Level Gateways or TCP Tunnels),也有人将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术,其特点是将所有跨越防火墙的网络通信分为两段。代理服务作用在应用层,它用来提供应用层服务的控制,起到内部网络向外部网络申请服务时中间转接的作用。内部网络只接受代理提出的服务请求,拒绝外部网络其他接点的直接请求。

代理服务是设置在 Internet 防火墙网关上的应用,是在网络管理员允许或拒绝的特定的应用程序服务,同时还用于实施较强的数据流监控、过滤、记录和报告等。

(4) 防火墙设置实例

在一台计算机中如何构建 Windows Server 2003 系统防火墙?如何完成对防火墙的启动、停止?如何设置相应的安全策略设置?

① 启用防火墙

打开网络连接的图标,选择该窗口中的“本地连接”,右击该图标,在弹出的快捷菜单中选择“属性”命令,系统将弹出“本地连接 属性”对话框,如图 7-8 所示。

在“本地连接 属性”对话框的“高级”选项卡中单击“Internet 连接防火墙”链接,启动 Windows 防火墙,如图 7-9 所示。

系统默认是关闭防火墙的。启动它之后,网络中的其他用户或者计算机访问系统将受到限制。



图 7-8 “本地连接 属性”对话框



图 7-9 启动 Windows 防火墙对话框

② 添加允许通过防火墙的服务和端口

在默认情况下，防火墙对于网络中的计算机和用户所提供的任何服务都不允许访问，例如如果使用远程桌面服务，就必须要在防火墙进行添加。

在“本地连接 属性”对话框的“高级”选项卡中，单击“设置”按钮，弹出“高级设置”对话框，如图 7-10 所示。

在该对话框中选择“远程桌面”复选框，单击“确定”按钮，这样网络中的其他计算机就可以使用远程桌面服务了。

如果“高级设置”中要添加新的服务或者应用程序，则可以单击“添加”按钮，弹出“服务设置”对话框，将需要添加的服务填写好即可，如图 7-11 所示。



图 7-10 “高级设置”对话框

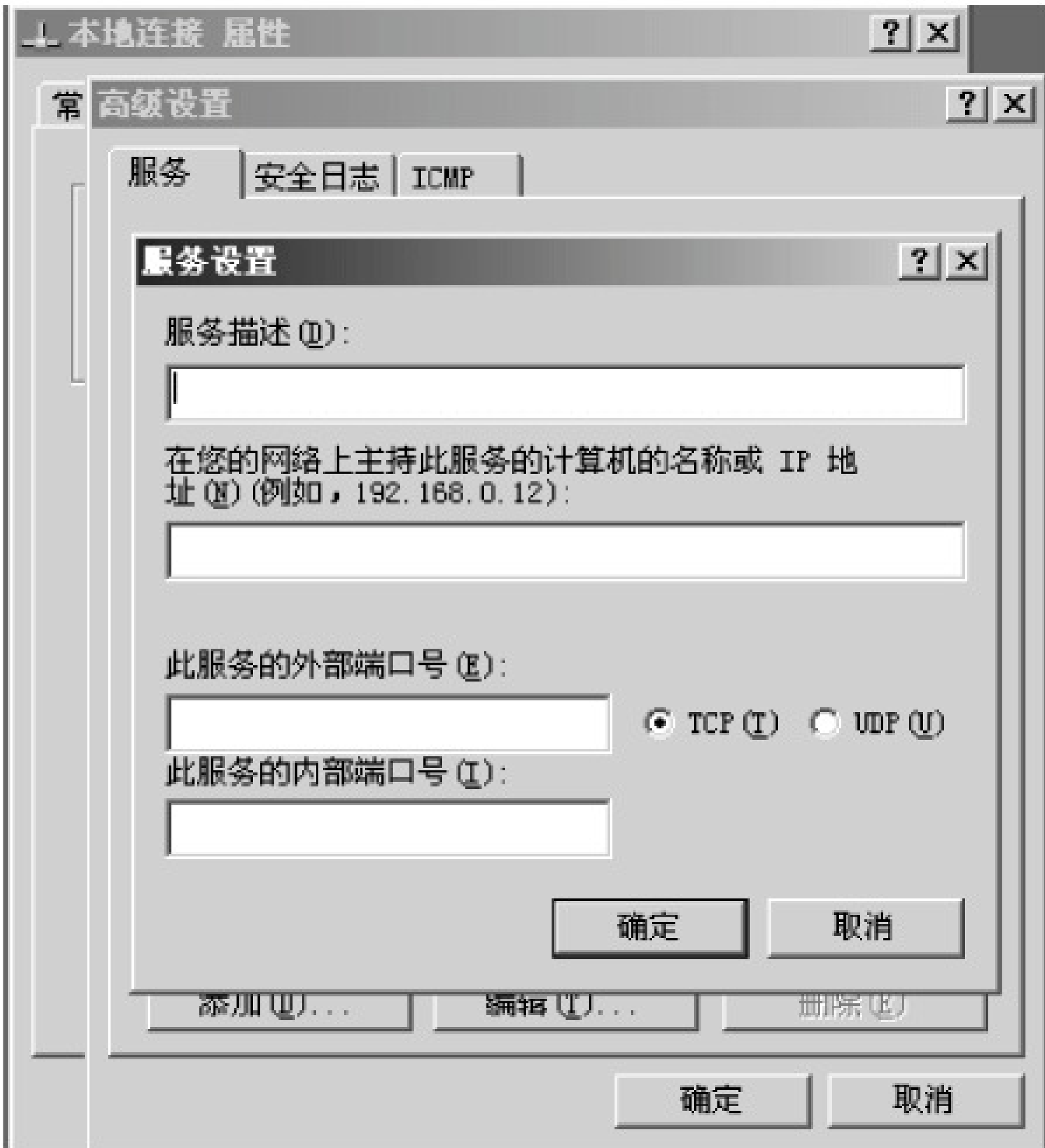


图 7-11 “服务设置”对话框

③ 添加允许通过防火墙的响应请求。

添加了 Web 服务后,虽然网络中的计算机和用户可以访问服务器的 Web 服务,但是要想在其他计算机中使用 ping 命令,默认情况下则会出现 Request timed out,表示目前该服务禁止。要想使用该服务则需要在“高级设置”对话框中打开 ICMP 选项卡,然后选择“允许传入响应请求”复选框,单击“确定”按钮即可,如图 7-12 所示。

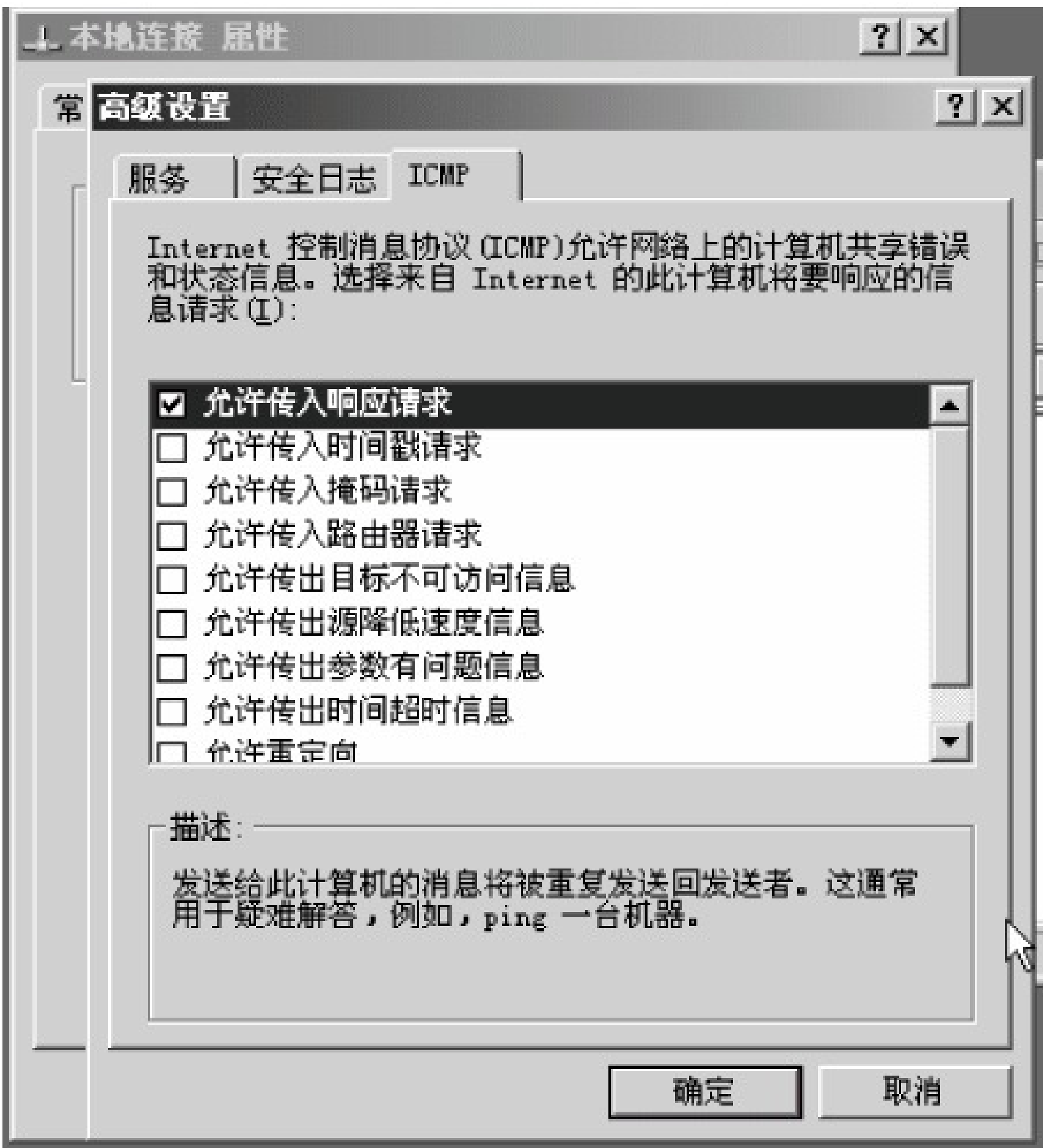


图 7-12 ICMP 选项卡

3. 身份认证技术

身份认证业务也称为鉴别验证业务。认证业务就是当某个实体用它的身份进行担保时,该业务将证实这一担保的正确性。我们所熟悉的用户名密码方式就是一种典型的身份认证技术。

身份认证技术是计算机网络安全保护的最基本措施,也是保障网络安全的第一道防线。目前常用的身份认证技术有:口令验证、通行证验证、人类特征验证。

(1) 口令验证

口令验证是验证用户的口令是否正确合法,是最基本的身份验证技术。

(2) 通行证验证

通行证验证是用凭证作为身份的识别证明,用户在使用时只需将此证件拿出来在识别器上进行识别即可。比如现在使用的各种磁卡。

(3) 人类特征验证

人类特征验证利用用户的生物特征或者是下意识的动作作为认证,这些特征具有很高的个性特征和防伪性,因此使用这种方法可靠性和准确性很高,但是鉴于成本方面的原因这种技术还没有广泛地使用。通常使用的人类特征有指纹、声音、视网膜、手写签名等。

任务 7.2 网络管理与故障排除

任务描述:某台计算机无法登录服务器,无法通过局域网接入 Internet,无法使用各种共享资源。检查本地配置及网络状态,进行适当设置,使其恢复正常。

7.2.1 网络管理简介

1. 网络管理的功能

网络管理功能一般分为故障管理、计费管理、配置管理、性能管理和安全管理 5 大管理功能。

(1) 故障管理

故障管理是网络管理中最基本的管理功能,主要工作是找出故障的位置并进行恢复。

其目标是自动监测、记录网络故障日志，对导致故障的条件进行响应，以便及时处理。

网络故障管理的具体操作步骤如下：

检测故障、判断故障症状：依赖于对网络设备的状态监测和检查差错日志。

隔离故障：通过跟踪、测试分析故障根源，对根源故障进行隔离。

故障修复：简单故障通常由网络设备通过本身具有的各种检测、诊断和恢复措施解决。复杂的故障要首先通过对网络设备的运行状况进行测试并记录测试的结果，由技术员分析和排查，再根据已有的对故障状态的描述给出对故障排除的提示。

记录故障的监测及其结果。

(2) 计费管理

计费管理负责记录网络资源的使用情况和用户在使用这些资源服务时需支付的代价。

(3) 配置管理

配置管理就是跟踪、收集、监测和管理系统的软硬件配置参数，并对网络配置的变化做出及时的响应。主要包括：配置信息的获取；配置信息的备份；配置信息的检查；配置信息的调整；配置信息的录入。

(4) 性能管理

性能管理主要收集、统计数据，以便规划和分析网络资源的运行状况和通信效率等系统性能，预测各系统之间的通信操作的趋势，或者平衡系统之间的负载。主要包括：数据采集；分析数据；阈值分析；实时监控等。

(5) 安全管理

对网络资源的访问方面的安全控制，保证网络不受非法用户的侵害，并保证重要的数据信息在存储和传输的过程中不被泄露、篡改和伪造。主要功能：根据网络要达到的安全等级，建立相应的身份认证、鉴别机制；用户分级管理与访问控制；系统日志的检查和维护，并对报警事件进行监测分析；系统安全漏洞检测，实时地监测网络系统的各个端口数据传输情况和重要的工作状态。

2. 网络管理系统协议

网络管理系统中最重要的部分就是网络管理协议，它定义了网络管理器与被管代理间的通信方法，目前主要网络管理协议是：SNMP(简单网络管理协议)和 CMIP(通用管理信息协议)。它们都使用管理信息库 MIB。MIB 中包含所有网络资源都遵循的信息、测试、公式和控制。

(1) SNMP 网络管理协议

SNMP 网络管理协议是一种专门在 TCP/IP 网络中使用的网络管理协议。该协议设计简单，实现过程容易，占用网络资源较少，便于应用。由于该协议应用广泛，网络设备商在生产网络设备时都加入了对 SNMP 协议的支持。SNMP 协议具有良好的可扩展性。

但 SNMP 协议存在一些安全漏洞，网络入侵者很容易获取正在通过网络传递的各种信息，设置可以关闭某些终端。SNMP 协议的最大问题是无法处理各种细节信息。

(2) CMIP 网络管理协议

CMTP 网络管理协议是由 ISO 为监视和控制多种网络而创建并标准化的 OSI 网络管理协议。

该协议的优势是所使用的变量可以像 SNMP 一样在网络管理系统和终端之间传递信息，还可以被用来执行各种 SNMP 不能实现的任务。

CMIP 可以及时向有关用户发出事件提示，从而避免在整个过程中的人工干预，简化了用户对网络的人工监控。

CMIP 内置了安全管理设备，支持验证、访问控制和安全日志等安全防范措施，它本身成为一种安全系统。

缺陷：CMIP 所占用的网络资源相当于 SNMP 的 10 倍。

3．局域网的数据管理

随着网络的发展，信息资源的安全问题成为关键。而数据是最重要的资源。网络数据管理要求不仅能立即访问准确信息，更重要的是要将综合存储作为组成部分。综合信息存储首要问题是数据资源的备份。

（1）备份分类

系统备份：用户使用系统备份功能进行自动备份，系统本身会自动创建还原点，用户也可以手工设置还原点。用户使用 Ghost 软件进行备份。有两种：一是使用 Ghost 管理器 Ghost.exe 对镜像中的部分内容进行及时更新；还有就是保持系统完整、配置基本稳定的情况下重新制作镜像文件。

资料备份：只要使用相应的管理软件即可。

文档备份：文档类数据备份，要做到及时更新备份文档。

（2）备份方法

① 使用备份向导备份与恢复数据。

备份文件和文件夹。

将数据备份到文件时，必须指定文件要保存的名称和位置。备份文件的扩展名为.bkf，也可以将扩展名自定义。步骤如下：

执行菜单命令“开始”→“所有程序”→“附件”→“系统工具”→“备份”，选择“高级”模式，出现如图 7-13 所示的对话框，单击“备份向导（高级）”按钮。

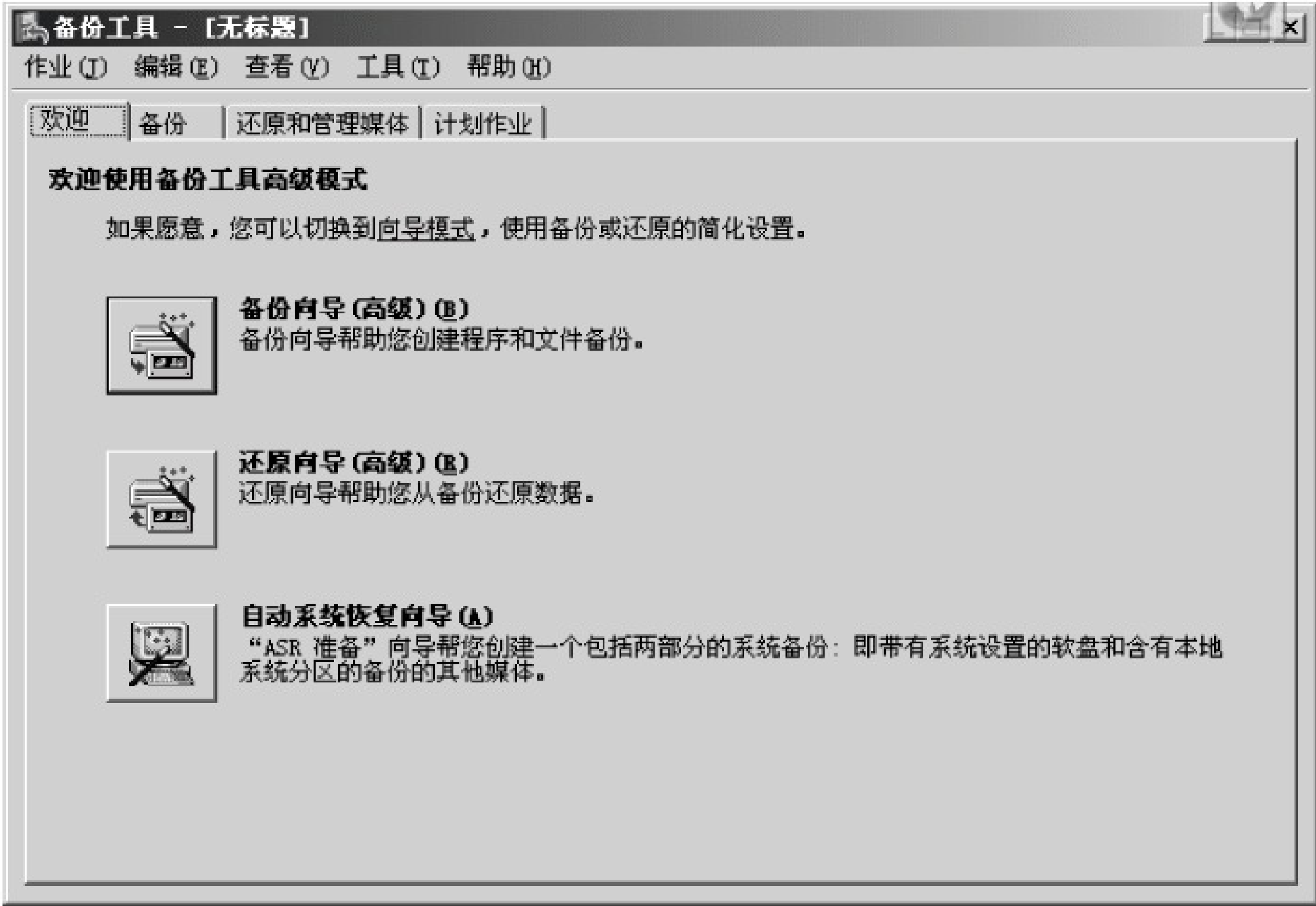


图 7-13　备份工具的高级模式

弹出如图7-14所示的对话框，选择“备份选定的文件、驱动器或网络数据”单选按钮。

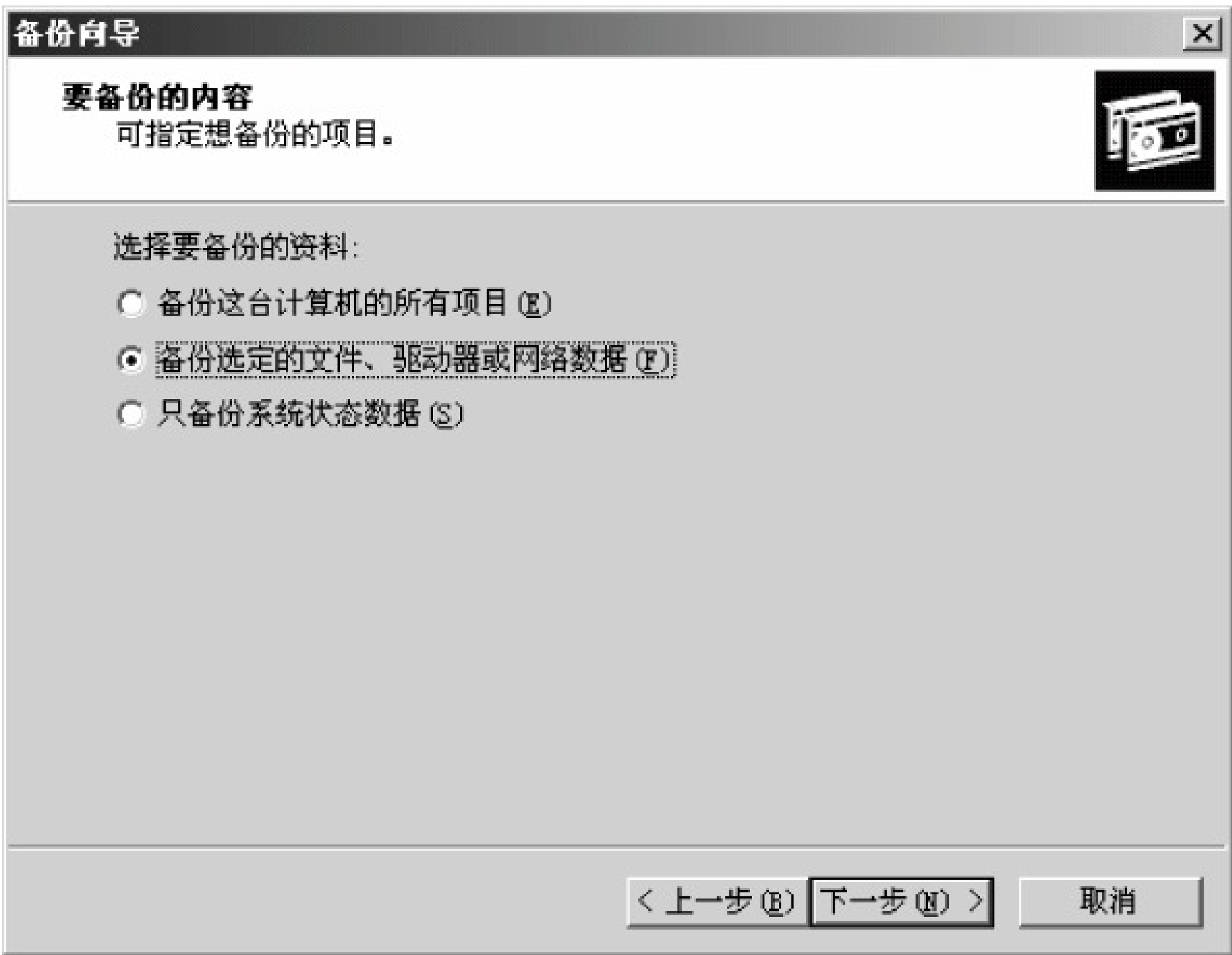


图7-14　备份内容选择

注意：系统状态数据是指由操作系统维护的系统特定的数据集合，必须将其作为一个单元进行备份，计算机需要系统状态数据来装载、配置和运行操作系统，包括注册表、启动文件、Registration数据库等。系统状态数据包含系统配置的大多数元素，但可能不包含用户对系统进行故障恢复时所需要的全部信息。因此，管理员在备份时应备份全部启动卷和系统卷。

选择要具体备份的文件和文件夹；输入保存备份文件的位置和备份文件的文件名；单击“高级”按钮，继续进行备份的高级设置，选择要采用的备份类型，如图7-15所示。

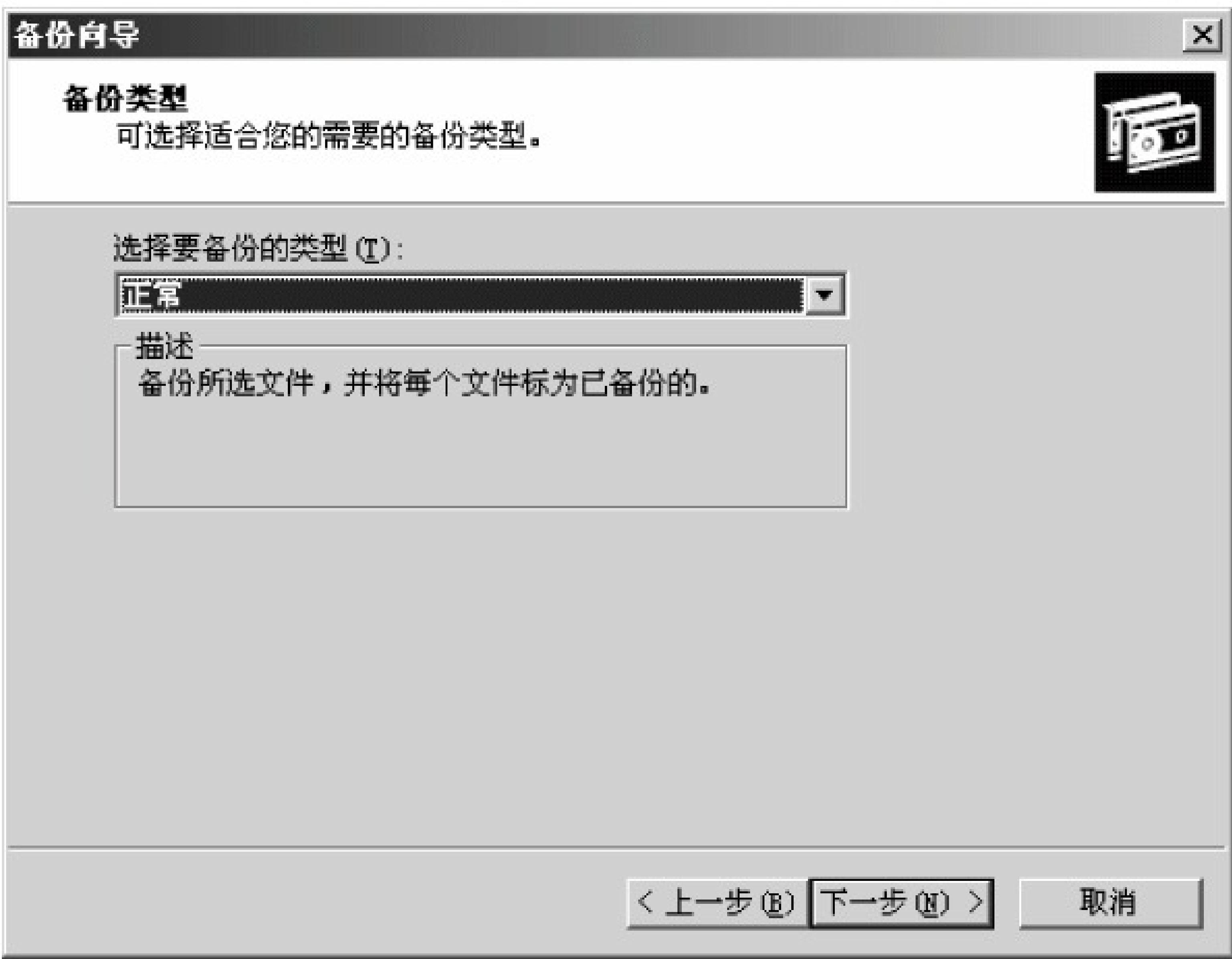


图7-15　备份类型

选择是否“备份后验证数据”；若是重要的数据，一般要验证。

选择“替换现有备份”。备份设置如图7-16所示。

说明：将这个备份加到现有备份（本次备份加到上次备份的数据后，保存在同一个备

份文件里)；替换现有备份(覆盖原来的备份数据)；只允许所有者和管理员访问备份数据，以及附加到这个媒体上的备份；只允许管理员和文件的所有者能够进行备份操作，替换原来的备份数据。

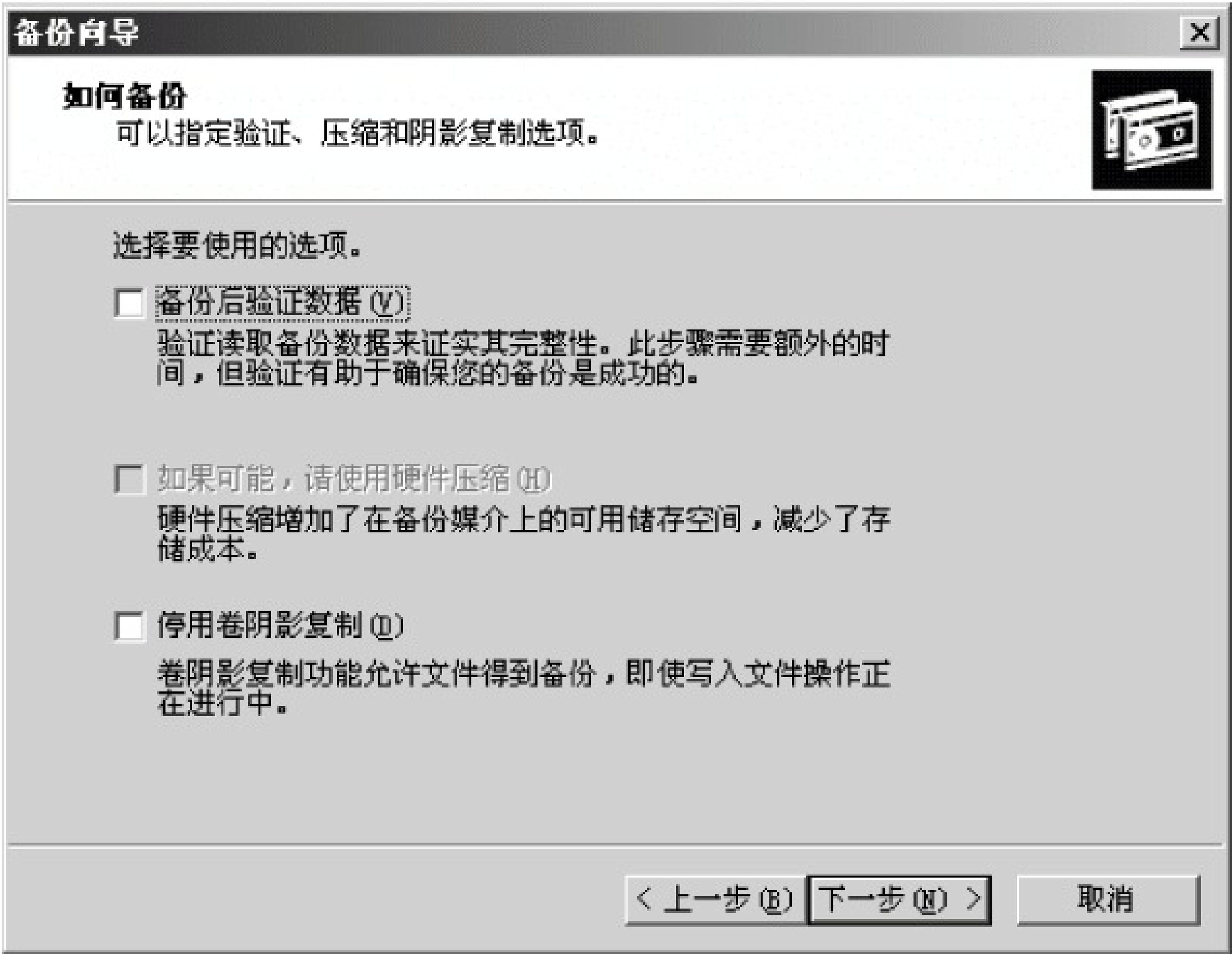


图 7-16　备份设置

系统开始备份数据，备份结束后，可以查看备份报告。

下面介绍还原备份数据的方法。

在“备份工具”对话框中，单击“还原向导”按钮，具体操作步骤是：

打开备份文件，选择要还原的文件和文件夹；选择要将文件和文件夹还原的位置。

注意：原位置：将备份文件和文件夹还原到原来的位置，用来恢复受到损坏或丢失的文件和文件夹，是最常用的选择。替换位置：将备份文件中的数据还原到另外一个文件夹中。单个文件夹：将备份文件还原到单一文件夹中，不保留原来文件夹的目录结构。

在如何还原界面中选择还原选项。说明：保留现有文件(若要还原的文件在当前已存在，则跳过该文件，不进行还原)；如果现有文件比备份文件旧，将其替换；替换现有文件。

在高级还原选项界面中选择使用的项。说明：还原安全设置(在 NTFS 卷中备份和还原时，保留原文件的初始权限)；还原交接点(不还原交接点引用的文件夹和文件数据)；保留现有卷的装入点(还原所有复制数据集的数据)。

单击“完成”按钮，按设置完成还原。

② 利用 Ghost 快速备份与恢复数据。

Ghost 是一个用于系统、数据备份与恢复的工具。使用 Ghost 进行系统备份，有整个硬盘和分区硬盘两种方式。可以用 Ghost 快速安装 Windows 操作系统，基本过程是：先将用户的系统分区做成一个扩展名为.gho 的镜像文件并保存在其他分区里，当需要重新安装 Windows 时，就可以利用这个镜像文件在短时间内还原系统(注意：至少有两个分区)。

接下来介绍如何备份数据。

备份分区的步骤如下。

在 Ghost 主菜单执行“Local→Partion→To Image”,选择存放镜像分区所在的硬盘;单击“下一步”按钮;选择将要克隆的分区(可以选择多于一个的分区进行克隆,按 Ctrl 键选择);设定镜像文件的保存位置和文件名,单击 Save 按钮;选择是否压缩该镜像文件;确定是否创建分区镜像文件。等待完成镜像文件的创建。

恢复分区的步骤如下:

在 Ghost 主菜单执行“Local→Partion→From Image”,选择镜像的文件;选择待恢复分区;选择目标硬盘,选择目标分区;确认后开始恢复镜像。

③ 利用 Symantec Ghost 快速恢复多机系统。

由于多种原因,在网络的维护和管理中,需要重新安装系统或单机做一个镜像来恢复。为了方便管理,可以利用 Symantec Ghost 进行网络服务器/客户端的映射克隆。

制作工作站启动盘的方法如下:

在“Ghost Cast 服务器”中,执行菜单命令“开始”→“程序”→Symantec Ghost→Ghost Boot Wizard,选择 Standard Ghost Boot Disk,单击“下一步”按钮;选择对应的机房网卡驱动程序;单击“下一步”按钮直到完成设置。

获取镜像文件的方法如下:

工作站的一台计算机安装并调试好所需操作系统和应用软件。在服务器中,执行菜单命令 “开始”→“程序”→Symantec Ghost→GhostCast Server,在 Session Name 中加入会话名(任意);选中 Create Image 项,在 Image File 栏中选择镜像文件存放的路径和镜像文件名;选择(硬盘克隆 DISK 还是分区克隆 Partition),在“Partition No.”栏确定是第几个分区;最后单击 Accept Clients 按钮,进入等待工作站端的接入;用制作好的工作站启动盘启动工作站样机进入 Ghost 窗口,选择 Ghost Cast/Multicast 打开与多播服务器的命名窗口,输入服务器端确定的会话名。单击“确定”按钮;选择目标硬盘和镜像文件的压缩比,即开始克隆。完成后则生成对应的镜像文件。

多机克隆的方法如下:

在服务器中,执行菜单命令 “开始”→“程序”→Symantec Ghost→GhostCast Server,在打开的窗口中,输入会话名;选中 Restore Image;单击 more Options 后,在 Auto Start 框内的 Client 栏输入要克隆的客户机的个数,最后单击 Accept Clients 按钮,加入等待工作站接入。依次启动要克隆的客户机,使之进入 Ghost 窗口,输入服务器端的会话名称,选择目标硬盘,最后进入等待接受数据状态。工作站的客户机启动到设定的台数,就自动开始多机克隆了。

7.2.2 常见的网络故障诊断工具

在网络系统中出现故障不可避免,要进行网络维护和网络故障诊断需要借助测线器、数字万用表、网络测试仪、网络命令和网络监视软件等工具完成。

1. 常用的网络测试硬件工具

测试仪:用来显示线缆问题以及 RJ-45 接头是否是好的工具。可以检测双绞线和 RJ-45 接头的以太网线路。该工具由两部分组成,分别连接网线的两端。若是测试较短

的线缆，可以直接将线缆的两端接入主测试器中，如果是较长的线路，线路的两端接头分别插入两块测试器中。

数字万用表：一般用来检查电源插座电压是否正常，测试 PC 电源，测试同轴电缆接头处的终端匹配器。

网络测试仪：提供了实时的网络分析测试。它将网络管理、故障诊断以及网络安装调试等功能集中在一个仪器中，它可通过网桥、路由器观察整个网络的状况。

2. 软件工具

常用的维护命令如下。

(1) IP 测试工具 ping

使用 ping 命令可以向计算机发送 ICMP(Internet 控制消息协议)数据包并监听回应数据包，以校验与远程计算机或本地计算机的连接；ping 还可以测试计算机名/域名和 IP 地址，如果能够成功校验 IP 地址却不能成功校验计算机名或域名，则说明名称解析存在问题。

命令格式如下：

```
ping [ - t] [ - a] [ - n count] [ - l size]
```

参数含义：

-t　不停地向目标主机发送数据，直到用户按 Ctrl+C 快捷键为止。

-a　以 IP 地址格式来显示目标主机的网络地址。

-n count　指定要 ping 多少次，具体次数由 count 来指定，默认值为 4。

-l size　指定发送到目标主机的数据包的大小，默认值为 32B，最大值为 65 527B。

-f　在包中发送“不分段”标志。则该数据包将不被路由器分段。

-i TTL　指数据包的生存时间，具体由 TTL 值确定。

-v TOS　将“服务类型”设为 TOS 指定值。

-r count　在记录路由中记录发出的报文和返回的报文的路由。最大是 9，最小是 1。

-s count　指定转发次数的时间戳由 count 值确定。

-j host-list　经过由 host-list 指定的计算机列表的路由报文。最大值为 9。

-k host-list　经过由 computer-list 指定的计算机列表的路由报文。最大值为 9。

-w timeout　以毫秒为单位指定超时间隔。

target_name　指定要校验连接的计算机。

注意：Request Timed Out：*表示对方主机可以到达 timeout，这种情况通常是为对方拒绝接受你发给它的数据包造成数据包丢失。大多数的原因可能是对方装有防火墙或已下线。*

Destination Net Unreachable：表示对方主机不存在或者没有跟对方建立连接。这里要说明一下 destination host unreachable 和 timeout 的区别，如果所经过的路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这时候会出现 timeout，如果路由表中连到达目标的路由都没有，那就会出现 destination host unreachable。

Bad IP address：表示可能没有连接到 DNS 服务器，所以无法解析这个 IP 地址，也可

能是该 IP 地址不存在。

Source quench received：出现的几率很少。它表示对方或中途的服务器繁忙无法回应。

(2) 测试 TCP/IP 协议配置工具 IPConfig

IPConfig 命令可用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。IPConfig 可以让我们了解自己的计算机是否成功地租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和默认网关，实际上是进行测试和故障分析的必要项目。

命令格式如下：

```
ipconfig [/? | /all | /renew
```

参数含义：

/?　显示帮助信息。

/all　显示所有配置信息。

/release　释放指定网络适配器的 IP 地址。

/renew　刷新指定网络适配器的 IP 地址。

/flushdns　清空 DNS 解析缓存。

/registerdns　刷新所有 DHCP 地址信息并重新注册 DNS 名称。

/displaydns　显示 DNS 解析缓存。

/showclassid　显示指定适配器的 DHCP ClassID。

/setclassid　设置指定适配器的 DHCP ClassID。

Adapter　网络适配器名称，即在系统网络连接中所看到的连接名称，支持？/ * 通配符。

执行 ipconfig /all 命令的结果如图 7-17 所示。



图 7-17　IPConfig 命令

(3) 跟踪工具 Tracert

tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器,以及每个跃点所需的时间。如果数据包不能传递到目标,tracert 命令将显示成功转发数据包的最后一个路由器。当数据包从我们的计算机经过多个网关传送到目的地时,tracert 命令可以用来跟踪数据包使用的路由(路径)。

命令格式如下:

```
tracert [ - d] [ - h maximum_hops] [ - j host - list] [ - w timeout] target_name
```

参数含义:

-d　不将 IP 地址解析到主机名称。

-h maximum_hops　在搜索目标的路径中指定跃点的最大数。

-j host_list　指定 tracert 程序中数据包所采用路径中的路由器的接口列表。

-w timeout　等待 timeout 为每次回复所指定的毫秒数。

target_game　目标主机名称或 IP 地址。

如在访问具体网站时,想知道从用户端到目的端(搜狐网)通过何种路径到达主页的,可在 DOS 系统下,输入命令 tracert www. sohu. com。

(4) netstat 命令

可以帮助网络管理员了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息,如显示网络连接、路由表和网络接口的信息,可以统计目前总共有哪些网络连接正在运行。命令可以显示所有协议的使用状态,包括 TCP 协议、UDP 协议以及 IP 协议等,另外还可以选定协议并查看其具体信息,还能表示所有主机的端口号以及当前主机的详细路由信息。

命令格式如下:

```
netstat [ - r][ - s][ - n][ - a][ - e]
```

参数含义:

-r　显示本机路由表的内容。

-s　显示每个协议的使用状态。

-n　以数字表格形式显示地址和端口。

-a　显示所有主机的端口号。

-e　显示以太网统计。

如图 7-18 所示为使用参数-n 的结果。

(5) route 命令

可以操作路由表,包括显示、建立和删除路由。

命令格式:

```
Route [ - f] [ - p] [command] [destination] [MASK netmask] [gateway] [METRIC metric] [IF
interface]
```

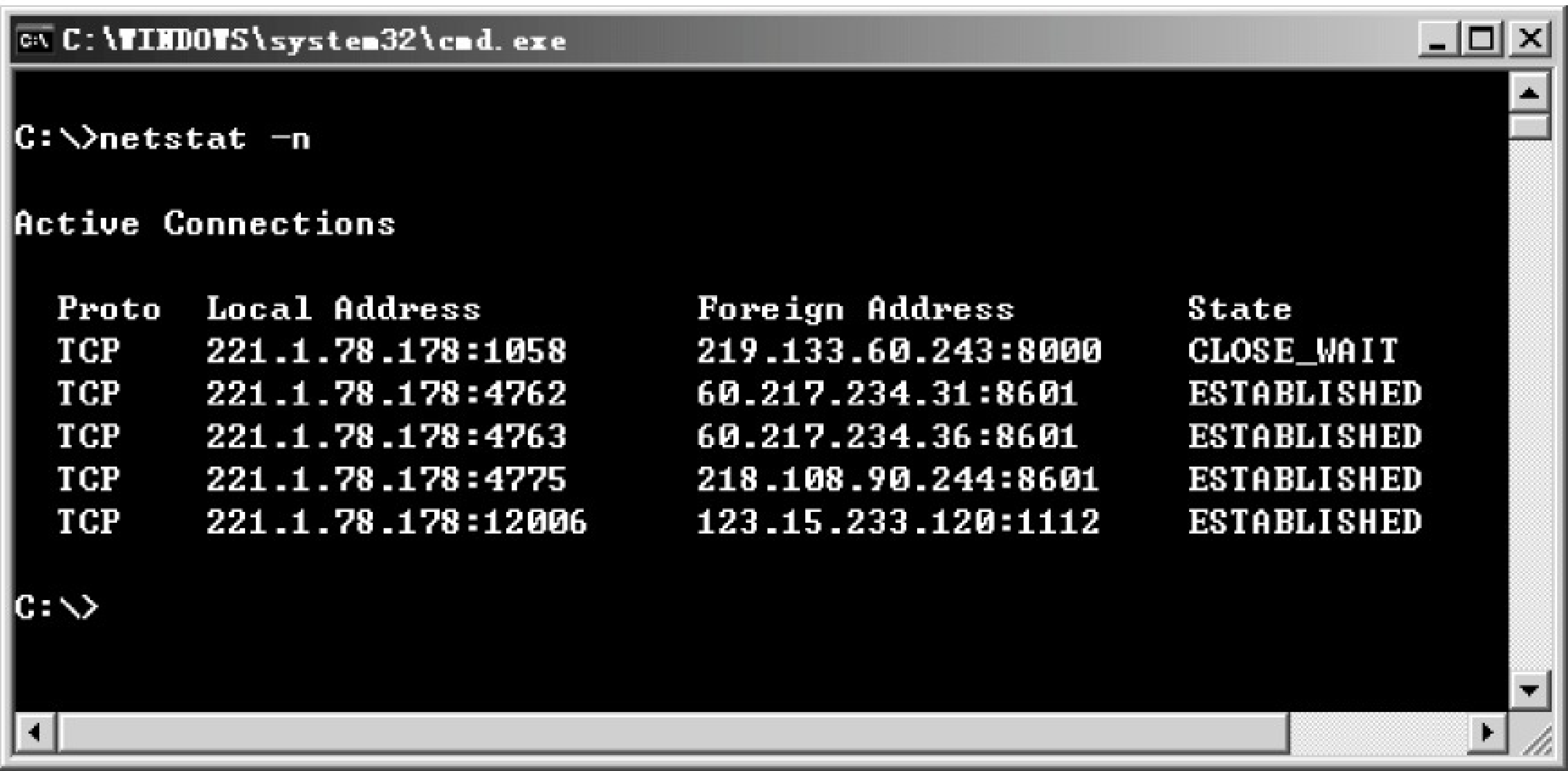


图 7-18　netstat 命令

参数含义：

-f　用于清除路由表。

-p　用于永久保留某条路由。

command 有 4 个命令　print(打印)、add(添加)、delete(删除)、change(修改)。

destination　目的 IP 地址。

netmask　代表具体的子网掩码。对于主机路由是 255.255.255.255，MASK 对应默认路由是 0.0.0.0。

gateway　代表出口网关 IP 地址。

如图 7-19 所示显示一个主机的路由表信息，根据这些信息可知本机的网关、子网掩码、广播地址、环回路测试地址等。

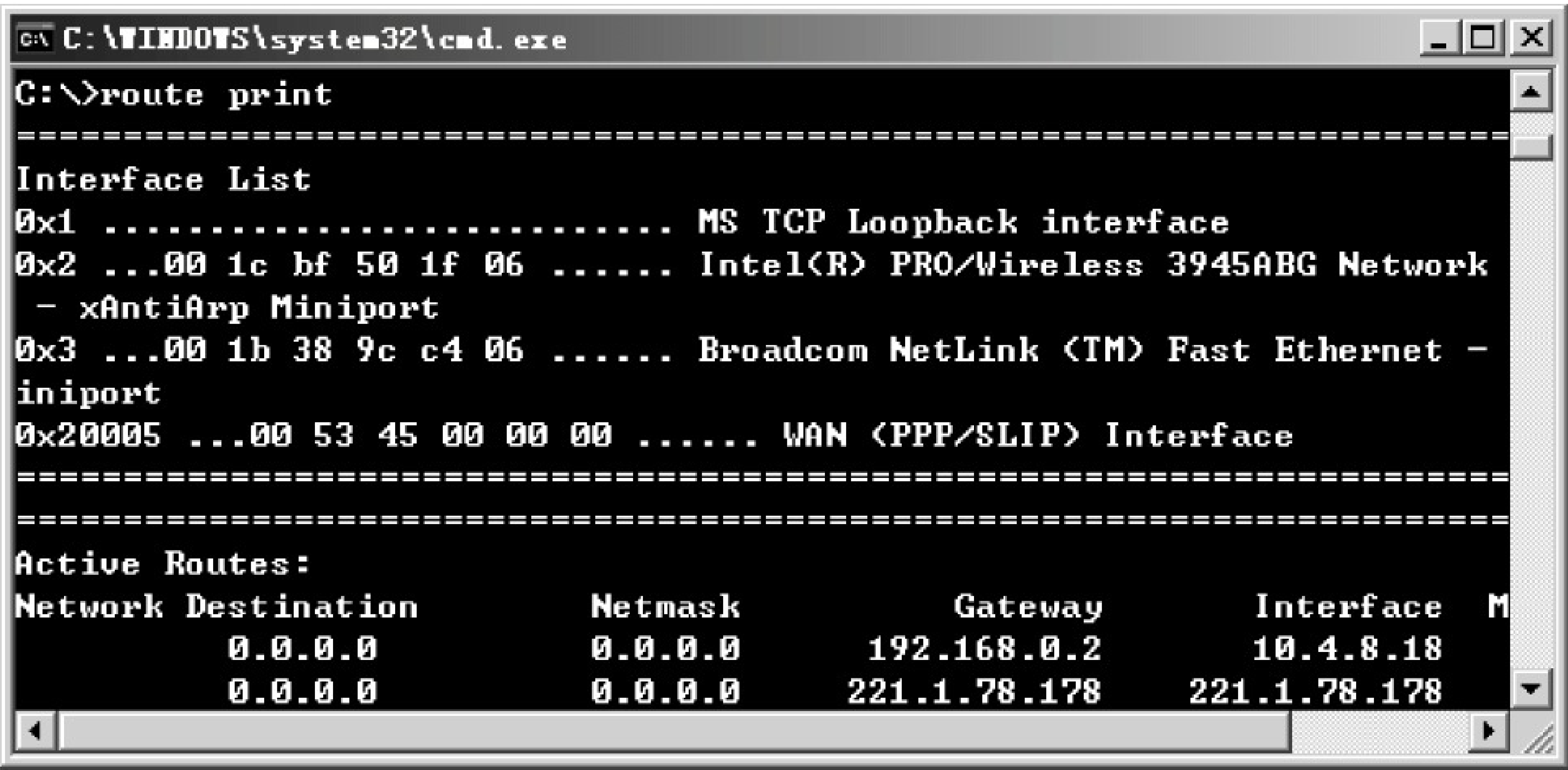


图 7-19　route print 命令

（6）解析工具 ARP

ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。显示和修改 ARP 缓冲区的内容，该缓冲区内存放 IP 地址和对应的 MAC 地址，即使用能够显示并修改 Internet 到以太网的地址转换表。

命令格式如下：

```
arp -s inet_addr eth_addr [if_addr];
arp -d inet_addr [if_addr];
arp -a [inet_addr] [-N if_addr];
```

其中：inet_addr 为 IP 地址；eth_addr 以太网卡地址。

参数含义：

-a　显示当前 ARP 高速缓存中的所有项目。如果已指定 inet_addr，则只是指定主机的 IP 地址和物理地址。如果有一个以上的网络接口使用 ARP，将显示各 ARP 中的内容。-a 可被视为 all，即为全部的意思。

-d　删除指定 IP 地址的主机，即能够人工删除一个静态项目。

-s　增加主机和与 IP 地址相对应的以太网卡地址。即向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

-f　读取一个给定名字的文件，根据文件中的主机名创建 ARP 表的项目。

网络监视软件：可以在连接到网络上的以太服务器或工作站上持续监测网络流量，它一般工作在 OSI 模型的第三层，它可以检测出每个包所使用的协议，但是不能破译包里的数据。

基于 Windows 的网络监视软件 Network Monitor，提供以下功能：从网络一段或几段中捕获传输数据；捕获出/入特殊节点的帧；通过发送指定数量和类型的数据来重视网络状态；检测在网络上的监视器的其他运行副本；产生网络活动的参数。

7.2.3　常见的网络故障

当今的网络互联环境是复杂的，而且其复杂性还在日益增长，主要原因如下：

现代的因特网络要求支持更广泛的应用，包括数据、语音、视频及它们的集成传输。

新的业务发展使网络带宽的需求不断增长，这就要求新技术的不断出现。新技术的应用同时还要兼顾传统的技术。

能够正确地维护网络尽量不出现故障，并确保出现故障之后能够迅速、准确地定位问题并排除故障，对网络维护和管理人员来说是个挑战。

这不但要求对网络协议和技术有着深入的理解，更重要的是要建立一个系统化的故障处理思想并合理应用于实际中，以将一个复杂的问题隔离、分解或缩减排错范围，从而及时修复网络故障。

故障处理系统化是合理地一步一步找出故障原因并解决的总体原则。它的基本思想是系统地将由故障可能的原因所构成的一个大集合缩减（或隔离）成几个小的子集，然后

分别处理这些小的子集,从而使问题的复杂度迅速下降。

当网络系统建立好了之后,在运行过程中,需要进行日常的维护、排除故障,保证系统的正常运行。下面介绍几种常见的网络故障。

1. 工作站故障

(1) IP 地址冲突

检查冲突主机的操作步骤如下。

① 更改自己的 IP 地址。

② 使用 ping 命令,确认非法使用 IP 地址的主机还在网络上。

③ 使用 nbtstat -a,确定机器的 MAC 地址和主机名。

④ 知道了主机名,就确定了是谁的 IP 地址强占了别人的 IP 地址。

如何预防 IP 地址冲突呢?

① 捆绑 MAC 地址和 IP 地址

在 DOS 命令提示符下,输入 IPConfig /all 命令,查出你的 IP 地址及对应的 MAC 地址。

例如:IP 地址为 10.10.17.8,MAC 地址为 00-E0-4C-A0-02-A4,则输入命令如下:

```
ARP-s 10.10.17.8 00-E0-4C-A0-02-A4
```

这样就把 MAC 地址和 IP 地址捆绑在一起了。

② 加强 IP 地址的管理

记录好 IP 地址及 MAC 地址等信息的记录,记录信息包括:主机名、分配的 IP 地址、网卡的 MAC 地址(在每台计算机上通过 IPConfig /all 命令可以得到)。另外就是要动态监视网络中的 IP 地址变化。

(2) 子网掩码设置不正确

在同一个网段中的计算机应该具有相同的子网掩码。如果子网掩码不同,就算位于同一个网段的计算机也是 ping 不通的。所以,出现同一网段的两台计算机不能互通的故障,除了要查看两台计算机的 IP 地址设置是否正确外,还要查看它们的子网掩码是否相同。

(3) 没有安装网络协议

TCP/IP 协议:是互联网协议,如果不安装该协议,网络是不能实现互联,也就无法上网,任何和互联网有关的操作都离不开 TCP/IP 协议。

是否安装了 TCP/IP 协议,也可以通过 ping 命令检测 TCP/IP 协议。

例如 ping 127.0.0.1(回测地址)看能否成功。

(4) 网关没有设置

不设置网关,同样是上不了网的。可以通过 TCP/IP 属性对话框来检查和设置。

(5) DNS 地址设置不正确

DNS 设置不正确,就不能对 IP 地址进行解析,也就无法使用域名进行访问网络,而只能使用 IP 地址进行网络访问。

假若在访问一个网站时,在浏览器中的 URL 地址框中,输入 IP 地址能够访问某一

网站，而输入域名就无法访问，首先检查是否设置了 DNS 地址，如果 DNS 地址设置没有问题，则大多是网站的域名服务器出现了问题。

2. 服务器故障

（1）服务器常见的故障及其排除方法

服务器中的某项服务被停止，大多是流量问题，系统资源不足，服务器软件故障。

其中服务器软件故障是在服务器故障中占有比例最高的部分，约占 70%。导致服务器出现软件故障的原因有很多，最常见的是服务器 BIOS 版本太低、服务器的管理软件或服务器的驱动程序有 BUG、应用程序有冲突或者是人为造成的软件故障。服务器软件设置不当也可能会造成网络故障。

（2）服务器故障排除的基本原则

① 尽量恢复系统默认配置。

② 从基本到复杂。首先将存在故障的服务器独立运行，待测试正常后再接入网络运行，观察故障现象变化并处理；然后从可以运行的硬件开始逐步到现实系统为止；最后从基本操作系统开始逐步到现实系统为止。

③ 交换对比。先在最大可能相同的条件下，交换操作简单效果明显的部件；其次是交换 NOS 载体，即交换软件环境；然后是交换硬件，即交换硬件环境；最后是交换整机，即交换整体环境。

在服务器故障排除时，需要收集如下一些信息。

服务器信息：机器型号（P/N）、机器序列号（S/N）、BIOS 版本、是否增加其他设备（如网卡、SCSI 卡、内存、CPU 等）、硬盘如何配置和安装什么操作系统及版本。

故障信息：在 POST（加电自检）时，屏幕显示的异常信息、服务器本身指示灯的状态和报警声，以及操作系统的事件记录文件等信息。

以 HP LH6000 服务器来说，有红、黄、绿三种指示灯，绿灯常亮表示服务器正常；绿灯亮而黄色闪烁表示服务器有故障，但不是致命的；如果红、黄、绿三灯闪烁就表示服务器有致命故障，服务器停止运行。指示灯只能提示比较笼统的故障。

确定故障类型和故障现象：开机无显示；上电自检阶段故障；安装阶段故障和现象；操作系统加载失败和系统运行阶段故障。

（3）服务器故障恢复

当服务器系统或用户操作错误而导致系统工作不正常甚至系统崩溃时，管理员可以使用一些系统还原的方法让系统恢复到正常状态。

① 使用安全模式恢复系统

常用于解决系统配制错误、硬件驱动程序错误等原因造成的操作系统无法正常启动的问题。有时也可以删除一些在正常模式下无法删除的文件。系统启动时按 F8 键打开“Windows 高级选项”菜单；选择一个合适的启动模式后，启动 Windows 操作系统（最常用的是“安全模式”和“最后一次正确的配置”）；系统启动成功后，可以通过修改注册表、修改系统配置、重新安装驱动程序等方法来解决系统故障。

② 故障恢复控制台

当使用安全模式也无法启动服务器时，可通过故障恢复控制台引导系统，并在故障恢

复控制台中尝试修复系统。只有系统管理员才能使用故障恢复控制台来引导系统，通过故障恢复控制台中的命令，可以启动或停止某项系统范围、读写本地磁盘的数据、从光盘或软盘复制数据、检修引导扇区或者主引导记录等。

使用故障恢复控制台的操作步骤如下。

插入 Windows Server 安装光盘，从光盘启动；按 R 键选择“修复或者恢复系统”，选择要修复的已安装的操作系统；输入管理员密码，进入故障恢复控制台。使用故障恢复控制台提供的命令来修复系统，具体命令格式可通过 help 命令查看。

3. 路由器的硬件故障

(1) 电源和冷却系统的故障

当接通电源时，电源指示灯亮。检查风扇是否正常工作。

若电源在启动后很快死机，则可能是环境过热引起的。路由器的工作环境温度应为 0℃～40℃。

若路由器无法启动，但电源指示灯亮，检查电源是否正常。

若路由器连续地或间歇地自动重启，可能是处理器或软件的故障，也可能是某条 DRAM 的安装不正确。

(2) 端口、电缆及连接的故障

若路由器无法确认某端口，检查电缆连接的是否正确。

当接通电源时，检查电源指示灯是否发亮。若不亮，检查电源及电源线。

若启动了系统，但屏幕没有反应，检查终端设置是否正确。

(3) 通过检查 LED 指示灯发现故障

指示灯显示路由器的目前的工作状态。通过观察指示灯，可以发现某些路由器的故障。

下面以 Cisco 2600 系列路由器为例来说明。

POWER 指示灯：显示路由器的工作状态。

冗余电源 RPS(Redundant Power System)指示灯：RPS 指示灯亮说明正常；RPS 指示灯闪动说明有错误。

ACTIVITY 指示灯：指示灯熄灭说明 Cisco IOS 操作系统已经运行，但没有网络活动；指示灯闪动，500ms 亮，500ms 灭，说明没有错误；若指示灯闪动，500ms 亮，500ms 灭，亮与灭之间间隔 2s，说明有错误出现；若指示灯闪动少于 500ms，说明操作系统软件已经运行，闪动的速率表明网络活动的水平。

LINK 指示灯：发亮时表明与线路另一端的集线器或交换机的连接已经建立。

ACT 指示灯：在 Ethernet 端口上正在传送或接收数据包。

FDX 指示灯：发亮时表示端口在全双工状态下，熄灭是在半双工状态下。

Mb/s 指示灯：发亮时表示端口速度为 100Mbps，熄灭时端口的速度为 10Mbps。

(4) 判断线路是否中断

DDN 线路。查看 DTU 的指示灯，DTU 上共有 4 种指示灯：Power、Line、DTR 和 Resdy。Power 指示灯在 DTU 上电后应保持长亮，而 Line 指示灯和 Ready 指示灯表示了该 DTU 与 DDN 节点设备连接的情况，正常情况下这两个指示灯也应该长亮。DTR

指示灯表示 DTU 与 DTE(路由器)的连接情况,当路由器上电后,若串口状态正常,则 DTU 上的 DTR 指示灯应保持长亮(当线路不通时,偶尔闪一下)。

模拟线路。查看 Modem 上的指示灯,一般对于同步专线来说,CD、TD、RD 应保持长亮,当有数据在广域网线路上传输时,TD 和 RD 指示灯将不停地闪烁。

4. 网络故障实例分析

故障表现:某台机器无法登录到服务器;也无法通过局域网接入 Internet;在“网上邻居”中只能看到自己,看不到其他计算机,从而无法使用其他计算机上的共享资源和共享打印机;无法在网络内实现访问其他计算机上的资源;网络中的部分计算机运行速度缓慢。

故障原因:网卡未安装,或安装不正确,或与其他设备有冲突;网卡硬件故障;网络协议安装或设置不正确;网线跳线或信息插座故障;Hub 电源未开、Hub 硬件故障,或 Hub 端口硬件故障;UPS 电源故障。

排除方法如下。

(1) 确认连通性问题,尝试其他网络应用,当其他网络应用也不正常,或用 ping 命令找不到其他机器,进入第(2)步。

(2) 查看 LED 灯判断网卡的故障。首先看灯是否正常,正常情况下,在不传送数据时,网卡的指示灯闪烁较慢,传送数据时,闪烁较快。不亮或长亮不灭,说明网卡有故障。

(3) 用 ping 命令排除网卡的故障,ping 本地的 IP 地址或计算机名,检查网卡和 IP 网络协议是否安装完好。如能 ping 通,说明协议和网卡都没有问题。问题出在计算机与网络的连接上。检查网线和 Hub 以及 Hub 的接口状态。如果 Ping 不通,说明 TCP/IP 协议有问题,可以在控制面板的系统窗口中查看网卡是否已经安装或是否出错。重新安装,并配置协议。若还不通,只能换网卡了。

若协议和网卡都正确,还是不通,只能初步判断是 Hub 和双绞线的问题,换一台计算机,如果正常,则故障出现在先前的计算机和 Hub 的接口上。

若确定 Hub 有问题,应先看指示灯,若接口指示灯不亮说明 Hub 的接口有故障。

若 Hub 无问题,测试双绞线。

通过上面的测试:可以判断故障出现在网卡、双绞线或 Hub 上。

知识拓展——网络安全立法

目前我国的主要计算机安全法规有:

(1) 1994 年我国第一部关于系统安全方面的法规《中华人民共和国计算机信息系统安全保护条例》。

(2) 1996 年发布的《中华人民共和国计算机信息网络国际联网管理暂行规定》。并于 1997 年 5 月 20 日根据《国务院关于修改〈中华人民共和国计算机信息网络国际联网管理暂行规定〉的决定》进行了修正。

(3) 1997 年 12 月 30 日发布的《计算机信息网络联网安全保护管理办法》。

(4) 2000 年发布的《计算机信息系统国际联网保密管理规定》。

国外的计算机安全立法有：

（1）美国的《信息自由法》、《可信计算机评价标准》、《可信网络说明》、《计算机安全法》。

（2）英国的《信息公开法》、《数据保护法案》、《个人资料获得法案》。

（3）国际组织：1996年联合国国际贸易法委员会公布了《电子商务范本》；1996年欧共体公布了《欧洲议会理事会关于资料库保护准则》；1997年欧洲联盟委员会公布了《欧洲电子商务：提案本》；1999年欧盟委员会拟订了《情报自由法草案》等。

实训7 防火墙配置

1. 实训目的

配置Windows XP自带防火墙。

2. 实训内容

Windows防火墙使用的全状态数据包检测技术，会把所有由本机发起的网络连接生成一张表，并用这张表跟所有的入站数据包做对比，如果入站的数据包是为了响应本机的请求，就允许进入。除非特例，所有其他数据包都会被阻挡。配置Windows XP自带防火墙，实现安全防护。

3. 实训步骤

（1）依次单击"开始"→"控制面板"→"Windows防火墙"进入防火墙配置界面。

（2）在"常规"选项卡中，设置防火墙的启停。

（3）在"例外"选项卡中，设置允许特定类型的传入通信，包括"添加程序"、"添加端口"、"编辑"、"删除"等操作。

（4）在"高级"选项卡用户可进行防火墙的进一步设置。

4. 实训要求

（1）启用防火墙，设置只允许腾讯QQ连接的规则，进行测试。

（2）设置不允许腾讯QQ连接的规则，进行测试。

习 题 7

1. 选择题

（1）下列关于计算机病毒的叙述中，错误的一条是（　　）。

A. 计算机病毒具有潜伏性

B. 计算机病毒具有传染性

C. 感染过计算机病毒的计算机具有对该病毒的免疫性

D. 计算机病毒是一个特殊的寄生程序

（2）下列关于计算机病毒的叙述中，正确的是（　　）。

A. 反病毒软件可以查、杀任何种类的病毒

B. 计算机病毒是一种被破坏了的程序

C. 反病毒软件必须随着新病毒的出现而升级,提高查、杀病毒的功能

D. 感染过计算机病毒的计算机具有对该病毒的免疫性

(3) 信息安全危害的两大源头是病毒和黑客,因为黑客是(　　)。

A. 计算机编程高手　　B. Cookies 的发布者

C. 网络的非法入侵者　　D. 信息垃圾的制造者

(4) 计算机病毒是一种特殊的(　　)。

A. 软件　　B. 程序、指令　　C. 过程　　D. 文档

2. 填空题

(1) 防火墙的技术包括 4 大类:________、________、________和________。

(2) 在网络应用中一般采取两种加密形式:________和________。

(3) CIH 病毒破坏计算机的 BIOS,使计算机无法启动。它是由时间条件来触发的,其发作的时间是每月的 26 号,这主要说明病毒具有________特性。

3. 简答题

(1) 简述网络安全的概念及其包含的内容。

(2) 网络安全防范的内容有哪些?

(3) 简述 ping 指令的功能和用途。

(4) Windows 防火墙如何禁用和启用?

模块8　案例分析——校园网的建设

任务8.1　功能需求分析

作为校园网,需要连接多少个节点,怎样使用各种网络设备使分布在不同地理位置的节点连接到一个统一的网络中,怎样使整个网络上的节点相互联通,这些问题仅仅是校园网需要解决问题中的一部分,更重要的问题是如何将这些资源有序地组织起来,需要实现什么功能,以满足现在和未来在教学、科研、管理、交流等方面的需求。形成在校园内部、校园与外部进行信息沟通的体系,建立满足教学、科研和管理需求的计算机环境,为学校各种人员提供充分的网络信息服务,在网络环境中进行教学、研究、收集信息等工作。

校园需要的基本功能有:

- 计算机教学,包括多媒体教学和远程教学。
- 网络下载、网络聊天等。
- 电子邮件系统:主要进行与同行交往、开展技术合作、学术交流等活动。
- 文件传输FTP:主要利用FTP服务获取重要的科技资料和技术文档。
- Internet服务:学校可以建立自己的主页,利用外部网页进行学校宣传,提供各类咨询信息等,利用内部网页进行管理,例如发布通知、收集学生意见等。
- 图书馆的接入系统,用于计算机查询、计算机检索、计算机阅读等。
- 其他应用,如网络化教学等。

任务8.2　网络结构设计

8.2.1　网络设计的基本原则

校园网建设是一项大型网络工程,各个学校需要根据自身的实际情况来制定网络设计原则。该学校网络需要完成包括图书信息、学校行政办公等综合业务信息管理系统,为广大教职工、科研人员和学生提供一个在网络环境下进行教学和科研工作的先进平台。校园网覆盖整个学校校园,网络设计一般应遵循下列8个基本原则。

1. 可靠性和高性能

网络必须是可靠的,包括网元级的可靠性,如引擎、风扇、单板、总计等;以及网络级的可靠性,如路由、交换的汇聚,链路冗余,负载均衡等。网络必须具有足够高的性能,满足业务的需要。

2. 实用性和经济性

由于学校资金并不是很充足,不可能一步到位。另一方面,学校的应用水平较参差不

齐，某些系统即使安装了也利用不起来，因此，在校园网的建设过程中，系统建设应始终贯彻面向应用、注重实效的方针，坚持实用、经济的原则。

3. 可扩展性和可升级性

系统要有可扩展性和可升级性，随着业务的增长和应用水平的提高，网络中的数据和信息流将按指数增长，需要网络有很好的可扩展性，并能随着技术的发展不断升级。设备应选用符合国际标准的系统和产品，以保证系统具有较长的生命力和扩展能力，满足将来系统升级的要求。

4. 易管理、易维护

由于校园骨干网络系统规模庞大，应用丰富而复杂，需要网络系统具有良好的可管理性，网管系统具有监测、故障诊断、故障隔离、过滤设置等功能，以便于系统的管理和维护。同时应尽可能选取集成度高、模块可通用的产品，以便于管理和维护。

5. 先进性、成熟性

当前计算机网络技术发展很快，设备更新淘汰也很快。这就要求校园网建设在系统设计时既要采用先进的概念、技术和方法，又要注意结构、设备、工具的相对成熟。只有采用当前符合国际标准的成熟先进的技术和设备，才能确保校园网网络能够适应将来网络技术发展的需要，保证在未来若干年内占主导地位。

6. 安全性、保密性

网络系统应具有良好的安全性。由于校园骨干网络为多个用户内部网提供互联并支持多种业务，要求能进行灵活有效的安全控制，同时还应支持虚拟专网，以提供多层次的安全选择。在系统设计中，既考虑信息资源的充分共享，更要注意信息的保护和隔离，因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括系统安全机制、数据存取的权限控制等。

7. 灵活性、综合性

通过采用结构化、模块化的设计形式，满足系统及用户各种不同的需求，适应不断变革中的要求。以满足系统目标与功能为目标，保证总体方案的设计合理，满足用户的需求，同时便于系统使用过程中的维护，以及今后系统的二次开发与移植。

8. QoS（质量服务）保证

教育在语音和视频等多媒体应用方面一直走在社会的前列，这类应用对服务质量的要求很高。QoS（质量服务）需要在网络的端到端进行全盘计划和实施，由于各接入网络和端设备的复杂性与多样性，骨干网必须尽可能地支持各种质量服务技术，特别是最新的技术如 MPLS VPN 和流量工程，以提供简洁透明的质量服务机制。

8.2.2 模块化、层次化的设计原则

网络的设计都是基于一个模块化、层次化的设计思想，这也是对大型网络进行高效管理的首选方法。

1. 模块化设计

所谓模块化就是把整个网络按功能和安全需求分为若干个组件，这些组件之间有一定的安全边界，组件内部有完整的网络设计。模块化设计的好处在于：

（1）解决各网络之间的冲突问题。

（2）简化安装和后台设备管理。

（3）易于故障检测和分离问题。

（4）易于执行不同类型的服务和安全方针。

（5）易于扩展和/或代替原来的技术。

一个完整的模块化网络设计模型如图 8-1 所示。

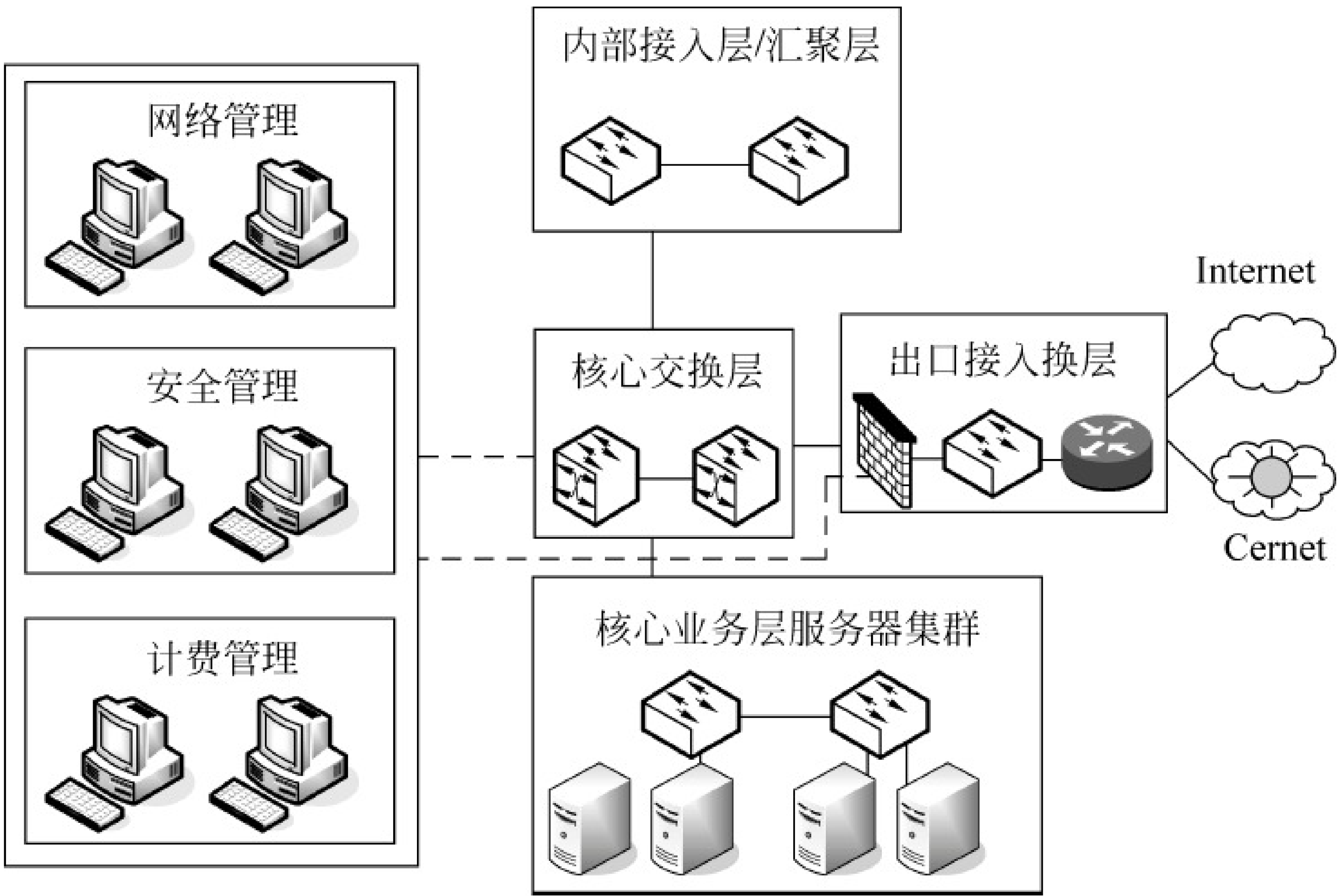


图 8-1　模块化网络设计模型

校园网的设计可以借鉴这种思想，对各种不同种类，不同安全等级的业务进行模块划分，相互之间的接入将受到控制。当然，在实际情况中并不一定要求严格按照上述模块划分，而是根据实际情况灵活运用，做适当的裁减与调整。

2. 层次化的设计

层次化网络设计模型对于大型网络，可以采用业界通用的“核心层—汇聚层—接入层”层次化网络设计模型。层次化网络设计模型如图 8-2 所示。

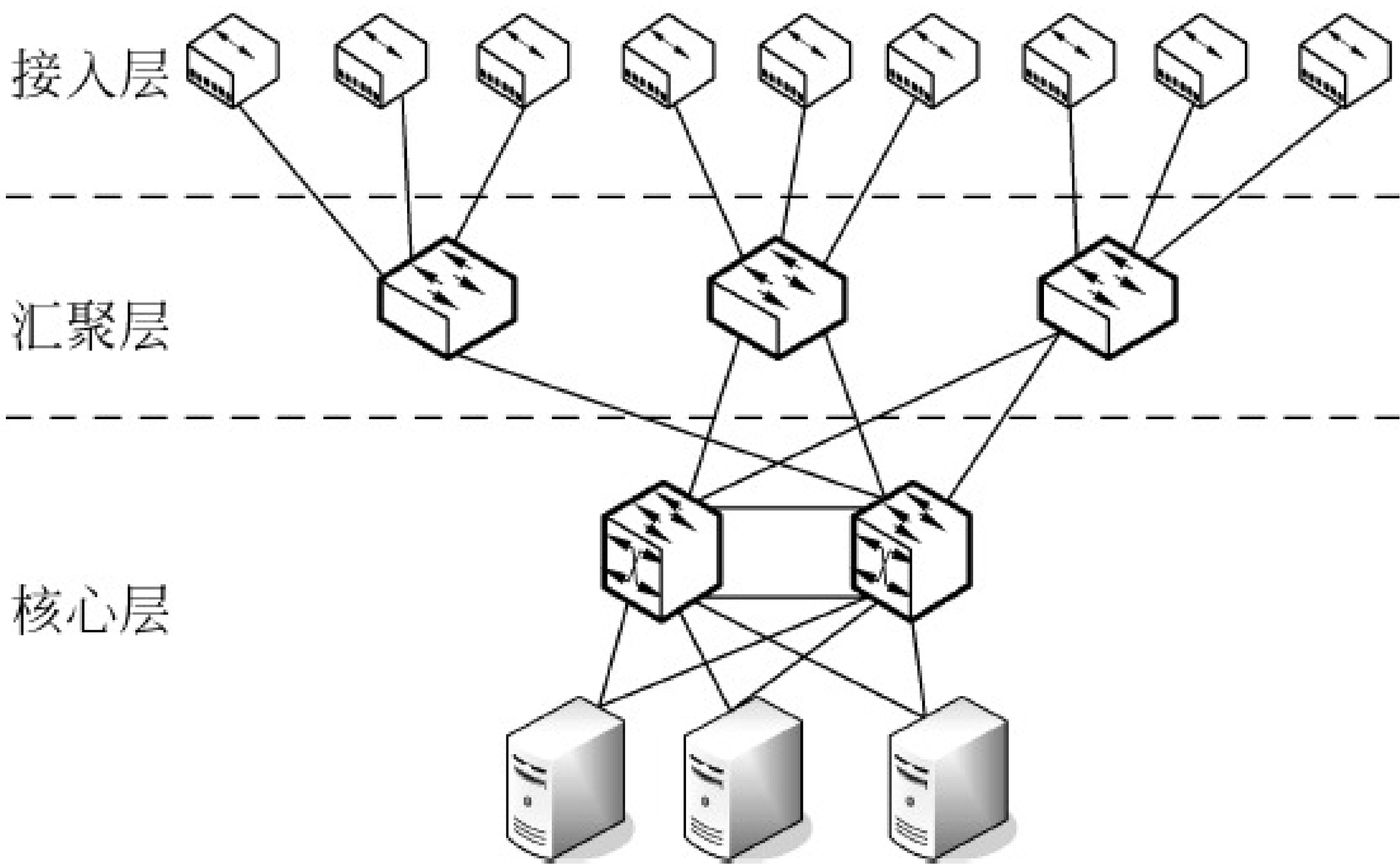


图 8-2　层次化网络设计模型

（1）核心层

核心层主要提供不同网络模块之间优化传输服务，将分组尽可能快地从一个网络传到另一个网络，通常要保证核心层具有很高的可靠性、最佳的网络性能，如图 8-3 所示。汇聚层到核心层要具备冗余传输链路，任何单条链路断连不影响网络的可用性。作为所有网络流量的传输中枢，核心层除了要求高性能交换设备和高带宽传输链路外，还需考虑选用支持负载均衡或负载分担特性的设备实现负荷均衡。此外，为了避免网元故障对网络造成冲击，需要网络采用支持快速聚合的特性，一旦主要通路断开，可以很快地切换到备用通路。

（2）汇聚层

汇聚层顾名思义就是作为接入层到骨干层的汇聚，通常为接入层与骨干层实现基于策略的网络间连接。汇聚层主要由三层交换机组成，提供对网络流量模式控制、服务接入控制、QoS、定义路由路径度量（Path Metric）和路由协议网络通告控制，如图 8-4 所示。

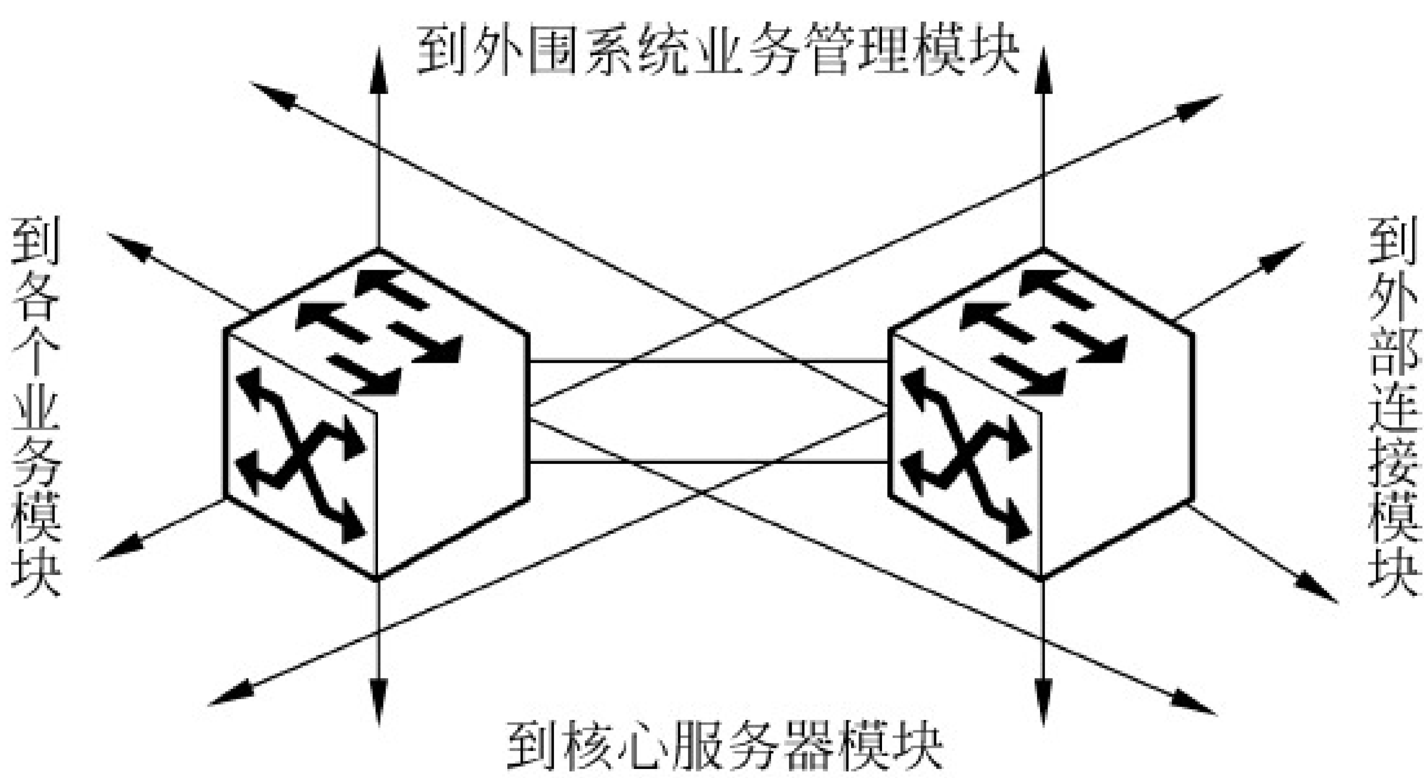


图 8-3　核心层网络模块

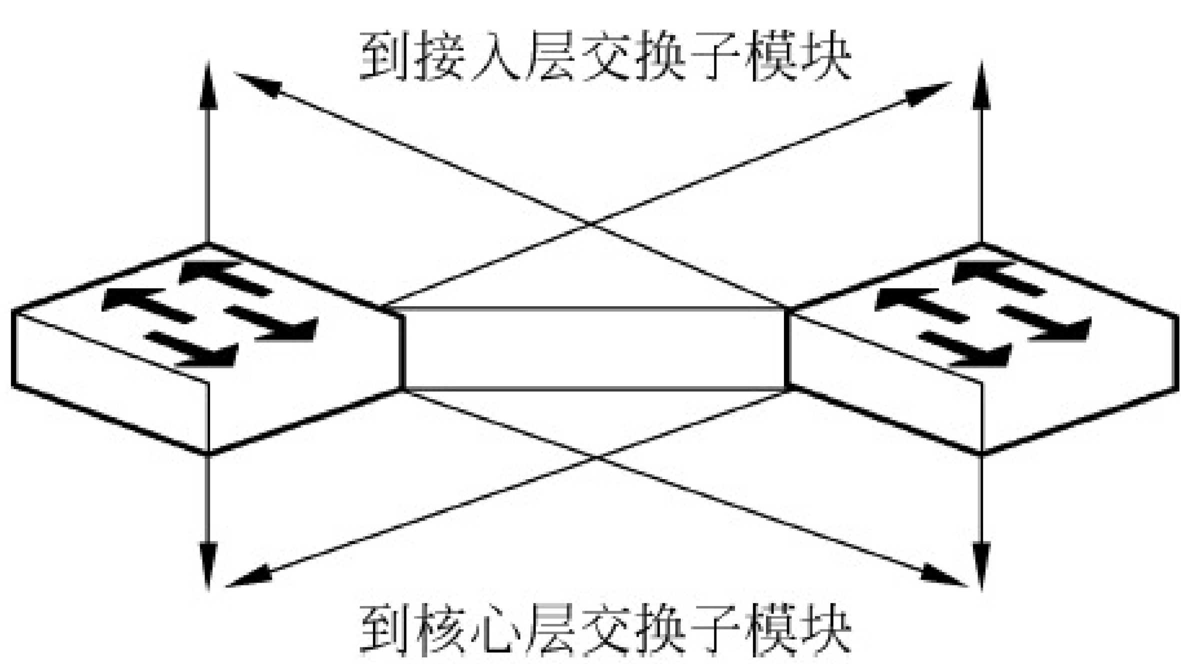


图 8-4　汇聚层网络模块

（3）接入层

接入层作为各模块到交换骨干的连接，根据不同模块进行逻辑子网划分，并通过 VLAN 技术实现子网之间的隔离。接入层主要功能在于隔离模块间的广播流量，避免不同模块之间相互影响。接入层主要通过二层交换机组成。

“核心层—汇聚层—接入层”层次化网络设计模型有如下优点。

① 高可扩展性。遵循层次化模型网络比扁平式网络更具有伸缩性和可管理性，因为各功能网络通过模块化实现，潜在问题更易于识别。

② 易于实施。每一层的功能性清晰划分，简化每一层的实现。

③ 易于故障排除。每一层的功能经过良好定义，网络更为简单，有助于故障的隔离。模块化设计也有效限制故障影响范围。

④ 易于规划和管理。层次化的功能划分，整个网络规划和管理更为简单。

8.2.3　设计方案及分析

本校园网设计案例是对实际校园网的设计进行了适当的和必要的简化。同时，将重点放在网络主干的设计上，对于服务器的架设只做简单介绍，具体内容可参考相关书籍。如图 8-5 所示，是该校园网网络的总体拓扑结构图。

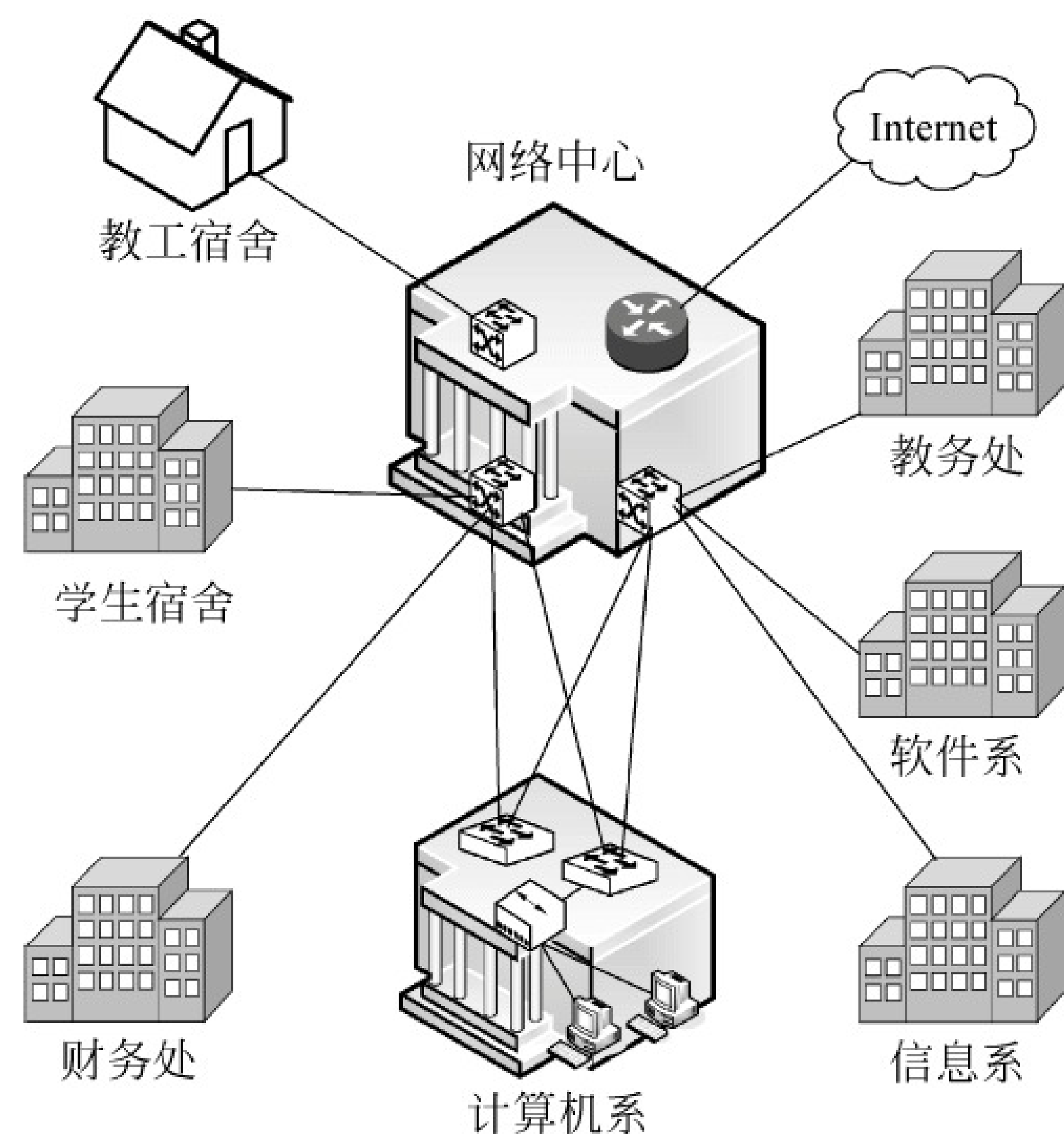


图 8-5　校园网网络的总体拓扑结构

在如图 8-5 所示的拓扑图中，学校的 6 个主要集中接入点(计算机系、管理系、建筑系、财务处、教务处、学生宿舍)通过冗余的光纤链路连到信息中心的核心层交换机上。核心层交换机通过 Cisco 3640 路由器接入因特网。此外，教工宿舍及移动办公用户通过拨号方式接入路由器 3640 来接入校园网内网及因特网。图 8-5 中，以计算机系为例展示了每个建筑物内部的网络设备拓扑结构，并给出了信息中心内部的网络设备拓扑结构。在接下来的讨论中，我们将展开并详细讨论每个模块的设计内容。

任务 8.3　设备需求分析

网络设备的选型是网络运行性能和售后服务的关键，根据实践经验，对于设备选型基于以下几点考虑。

(1) 网络中心的中心设备，承担着整个网络性能好坏的关键，我建议选用比较高档的中心设备，既能保证满足服务的需要，不会出现广播风暴或通信“瓶颈”问题；又能保证几年之内设备不会过时。

(2) 选择品牌时考虑比较多的是：生产厂商的可靠性和稳定性、技术领先性和成熟性、设备的完整系列性、设备的可升级性、是否具备完善的售后服务体系来支持用户的应用、是否为主流产品、在国内是否有比较完备的备件库和维护维修能力、其安全性是否适合用户的要求。

为了实现网络设备的统一，本设计方案中完全采用同一厂家的网络产品，即 Cisco 公司的网络设备构建。全网使用同一厂商设备的主要好处在于可以实现各种不同网络设备功能的互相配合和补充。本校园网设计方案主要由以下 4 大部分构成：交换模块、广域

网接入模块、远程接入模块、服务器模块。

任务 8.4　结构化布线

8.4.1　综合布线需求分析

计算机网络综合布线要完成的系统功能包括：

(1) 在网络系统范围内实现信息资源共享。

按照总体目标，系统将分级建设和逐步完善，最终实现网络系统的信息共享和数据、文本、语音、图像等各类信息的传输。

(2) 实现网络系统内网点信息传输，保证其高清晰度的图像传输。

(3) 满足各教室、办公室联网的需求。

(4) 具有较强的安全性和稳定性。

(5) 具有良好的可扩充性。

系统研制开发采用模块化设计思想，在实际工作中，可以根据不同需要以及工作性质、工作方法的变化进行调整和补充。

综上所述，计算机综合布线系统应该是易使用、易维护、高速稳定可靠性强的实用管理系统。

该案例的综合布线系统由工作区子系统、水平子系统、管理子系统和设备间子系统构成，充分考虑了高度的可靠性、高速率传输特性、可扩充性和系统易升级性，其信息点的分布依建筑物内的布线设计。下面分别对整个布线系统的 4 个子系统进行逐一描述。

8.4.2　结构化布线

1. 工作区子系统

工作区子系统由终端设备连接到信息插座的连线组成，在工程中涉及的工作区器件为信息插座。信息插座的选型采用 AMP 单孔面板。这种面板可以将语音和数据统一分配在同一个工作区域内，进行统一的管理。

2. 水平子系统

水平子系统是从配线间或跳线面板到独立的工作站或工作组之间的连线。水平子系统在办公区通过线槽将线缆从分配线间引至房间附近，再穿管引至信息出口。工程中涉及的水平子系统器件为超 5 类双绞线：所选的这种双绞线的传输要求已被 EIA/TIA-568A 标准所定义，这种双绞线适合那些传输频率可能达到 100MHz 的应用，并且超过了 EIA/TIA-568A 规定的 5 类扩展频率值。

3. 管理子系统

管理子系统提供与其他子系统连接的手段，使整个综合布线系统及其连接的设备、器件等构成一个有机的整体。管理子系统通常设置在配线设备的房间内，通常由配线硬件、输入/输出(I/O)设备等构成。

4. 设备间子系统

设备间子系统指设备间内与设备有关的系统。EIA/TIA569 标准规定了设备间的设备布线,它是布线系统最主要的管理区域。设备间是在每一幢大楼的适当地点设置进出线设备、网络互联设备的场所。

配线间是管理子系统的安装场所。其位置最好选择在有弱电竖井通过的房间内。配线间用于安装配线架和计算机网络设备,配线间应做到如下要求。

- 具有一定的亮度。
- 防尘且具有良好的通风性。

8.4.3 布线特点

1. 模块化

扩充的工作非常简单,因为在星型的结构中,工作站是由中心节点向外辐射,同时由于每一连线至节点的线路均与其他的线路相独立,故在执行更改或重新配置时,仅会影响到实际进行修改的线路。另外,此种结构可以使故障分析的工作变得非常简便,当有故障出现时,可以迅速地找出其位置并予以排除。

星型结构具有多元化的功能,可以让您在网络中搭配其他种类的结构一起运用。例如:局域网(LAN)通常使用总线结构,在各设备之间的信号传输是经由单一的途径到各设备或是使用环状结构。您只要在适当的节点上进行一些配线上的更动,即可将电路信号带入至任一结构上,而不需要移动缆线及设备。

2. 灵活性

本布线系统有自己的特色,是一种灵活的配线系统。

该系统可与其他厂商不同的产品一起结合使用。它不会使您局限于仅能使用唯一厂商的产品,还可以搭配其他厂商的产品而组成完整的网络系统。

该系统的灵活性组合提供服务与管理方面的最大方便性。由于其便于使用铜线,所以可以方便客户自行进行布线系统上线路的更改及管理,并可减少办公室搬动时在线路的布放及管理上所耗费的金钱与时间。

3. 开放性

本方案的布线系统可以综合所有数据通信设备上的布线。诸如 DEFINITY 通信系统 Genericl/System 75,信息系统网络(ISN)、DATAKIT II Virtual Circuit Switch 以及 StarLAN/StarWAN,虽然 SYSTIMAX PDS 为 AI&T 的标准系统,但是其适用性足以与其他的系统结合使用。

任务 8.5 网络配置与测试

8.5.1 IP 地址规划及 VLAN

在一个大中型网络里,VLAN 的划分是必不可少的步骤之一。在本校园网设计实例中,整个校园网中 VLAN 及 IP 编址方案如表 8-1 所示。

表 8-1　VLAN 及 IP 编址方案

VLAN 号	VLAN 名称	IP　网　段	默 认 网 关	说　明
VLAN1	—	192.168.0.0/24	192.168.0.254	管理系
VLAN10	JWC	192.168.1.0/24	192.168.1.254	教务处
VLAN20	XSSS	192.168.2.0/24	192.168.2.254	学生宿舍
VLAN30	CWC	192.168.3.0.24	192.168.3.254	财务处
VLAN40	JSJ	192.168.4.0/24	192.168.4.254	计算机系
VLAN50	RJ	192.168.5.0/24	192.168.5.254	软件系
VLAN60	DZ	192.168.6.0/24	192.168.6.254	电子系
VLAN70	XX	192.168.7.0/24	192.168.7.254	信息系
VLAN100	FWQ	192.168.100.0/24	192.168.100.254	服务器群

除了表 8-1 中的内容外，拨号用户从 192.168.200.0/27 中动态取得 IP 地址。为了简化起见，除了管理 VLAN 外，这里只规划了 8 个 VLAN，同时为每个 VLAN 定义了一个由拼音缩写组成的 VLAN 名称。

8.5.2　交换模块设计

一个好的校园网设计应该是一个分层的设计。一般分为三层设计模型。为了简化交换网络设计、提高交换网络的可扩展性，在园区网内部数据交换模块的部署是分层进行的。园区网数据交换设备可以划分为三个层次：接入层、汇聚层、核心层。传统意义上的数据交换发生在 OSI 模型的第二层。现代交换技术还实现了第三层交换和多层交换。高层交换技术的引入不但提高了园区网数据交换的效率，更大大增强了园区网数据交换的服务质量，满足了不同类型网络应用程序的需要。

现代交换网络还引入了虚拟局域网(Virtual LAN，VLAN)的概念。VLAN 将广播域限制在单个 VLAN 内部，减小了各 VLAN 间主机的广播通信对其他 VLAN 的影响。在 VLAN 间需要通信的时候，可以利用 VLAN 间路由技术来实现。

当网络管理人员需要管理的交换机数量众多时，可以使用 VLAN 中继协议(Vlan Trunking Protocol，VTP)简化管理，它只需在单独一台交换机上定义所有 VLAN。然后通过 VTP 协议将 VLAN 定义传播到本管理域中的所有交换机上。这样，大大减轻了网络管理人员的工作负担和工作强度。当园区网的交换机数量增多、交换机间链路增加时，交换网络的复杂性可能会造成交换环路问题，这需要通过在各交换机上运行生成树协议(Spanning Tree Protocol，STP)来解决。

1. 接入层交换服务的实现——配置接入层交换机

接入层为所有的终端用户提供一个接入点。这里的接入层交换机采用的是 Cisco Catalyst 2950 24 口交换机(WS-C2950-24)。该交换机拥有 24 个 10/100Mbps 自适应快速以太网端口，运行的是 Cisco 的 IOS 操作系统。这里以图 8-6 中的接入层交换机 AccessSwitch1 为例进行介绍。

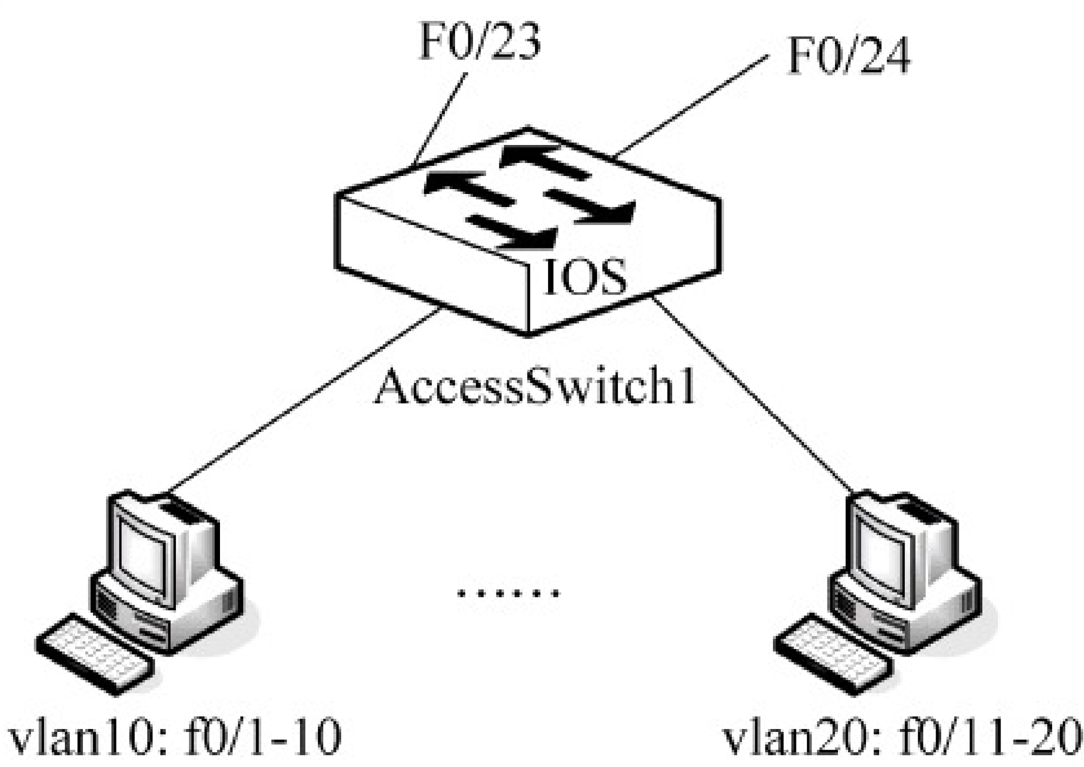


图 8-6　接入层交换机 AccessSwitch1

为接入层交换机 AccessSwitch1、AccessSwitch2 配置基本参数，包括设置交换机名称、管理 IP、默认

网关、VLAN 及 VTP、接入端口、主干道端口以及其他可选配置；例如基交换机名称、密码等的配置可以利用超级终端登录交换机的操作系统，运行下面命令。其他配置详细过程这里不再赘述。

```
switch>enable                                   ;进入特权模式
switch#config terminal                          ;进入全局配置模式
switch(config)#hostname <hostname>              ;设置交换机的主机名
switch(config)#enable secret ×××                ;设置特权加密口令为×××
switch(config)#enable password ×××              ;设置特权非密口令为×××
switch(config)#line console 0                   ;进控制台口(Rs232)初始化
switch(config-line)#line vty 0 4                ;进入虚拟终端 virtual tty
switch(config-line)#login                       ;允许登录
switch(config-line)#password ××                 ;设置登录口令××
```

2. 汇聚层交换服务的实现——配置汇聚层交换机

配置汇聚层交换机 DistributeSwitch1 与 DistributeSwitch2 的基本参数管理 IP、默认网关、VTP、端口基本参数，主要是在汇聚层交换机 DistributeSwitch1 上定义 VLAN，配置三层交换功能，以及其他配置。交换机 VLAN 及 VTP 的配置命令如下：

```
switch#vlan database                                    ;进入 VLAN 设置
switch(vlan)#vlan 2                                     ;建 VLAN 2
switch(vlan)#no vlan 2                                  ;删 VLAN 2
switch(config)#int f0/1                                 ;进入端口 1
switch(config-if)#switchport access vlan 2              ;当前端口 1 加入 VLAN 2
switch(config-if)#switchport mode trunk                 ;设置为干线
switch(config-if)#switchport trunk allowed vlan 1,2     ;设置允许的 VLAN
switch(config-if)#switchport trunk encap dot1q          ;设置 VLAN 中继
switch(config)#vtp domain <name>                        ;设置发 vtp 域名
switch(config)#vtp password <word>
switch(config)#vtp mode server
switch(config)#vtp mode client
```

3. 核心层交换服务的实现——配置核心层交换机

对核心层交换机 CoreSwitch1 与 CoreSwitch2 的配置除了基本参数配置外，还包括 VLAN 及 VTP、路由功能以及其他配置。路由配置命令如下：

```
CoreSwitch1(config)#ip routing
CoreSwitch1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.254
```

8.5.3 广域网接入模块设计

在本实例设计中，广域网接入模块的功能是由广域网接入路由器 InternetRouter 来完成的。采用的是 Cisco 的 3640 路由器。它通过自己的串行接口 serial 0/0 使用 DDN (128K)技术接入 Internet。其作用主要是在 Internet 和校园网内网间路由数据包。除了完成主要的路由任务外，利用访问控制列表(Access Control List，ACL)和广域网接入路由器 InternetRouter 还可以用来完成以自身为中心的流量控制和过滤功能并实现一定的安全功能。

对接入路由器 InternetRouter 的基本参数的配置步骤与对访问交换机 AccessSwitch1 的基本参数的配置类似，其他如接口参数、路由功能、NAT、访问控制列表 ACL 以及其他配置，已经超出本书范围，这里不再给出。

8.5.4　服务器模块设计

服务器模块用来对校园网的接入用户提供各种服务。在本设计实例中，所有的服务器被集中到 VLAN100，构成服务器群并通过分布层交换机 DistributeSwitch1 的端口 fastethernet 1～20 接入校园网，如图 8-7 所示。

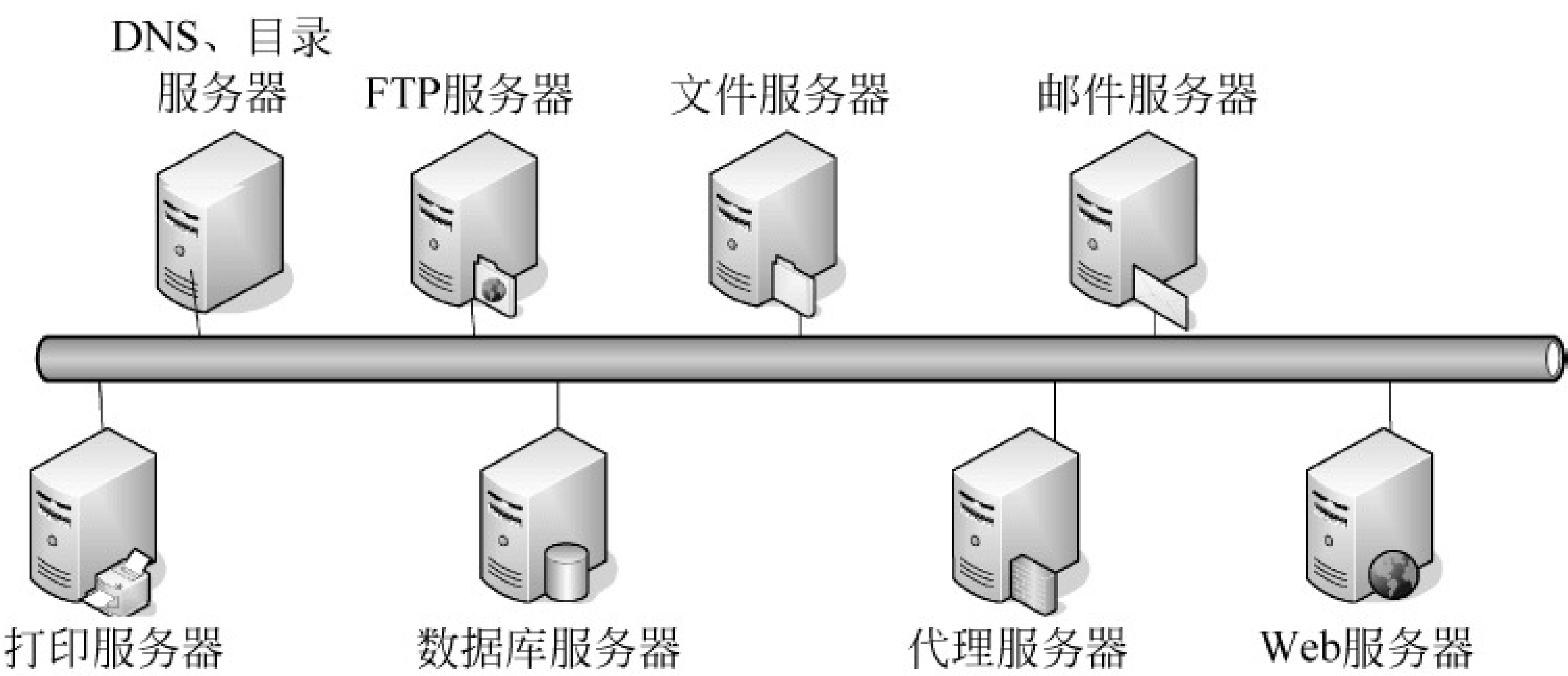


图 8-7　服务器群

校园网网络提供的常用服务（服务器）包括：

- Web 服务器：提供 Web 网站服务。
- DNS 目录服务器：提供域名解析以及目录服务。
- FTP 文件服务器：提供文件传输、共享服务。
- 邮件服务器：提供邮件收发服务。
- 数据库服务器：提供各种数据库服务。
- 打印服务器：提供打印机共享服务。
- 实时通信服务器：提供实时通信服务。
- 流媒体服务器：提供各种流媒体播放、点播服务。
- 网管服务器：对校园网网络设备进行综合管理。

表 8-2 给出了所有的服务器硬件平台、操作系统以及服务软件的选型表。限于篇幅，对于各种服务器的安装、配置步骤以及运行维护方法，这里不再赘述。感兴趣的读者可以参看有关参考书。

表 8-2　服务器硬件平台、操作系统以及服务软件的选型表

服务器编号	服务器名称	硬件平台	操 作 系 统	服 务 软 件
Server1	Web 服务器	HP LH3000	Window Server 2003	IIS 6.0
Server2	FTP 服务器	HP LH3000	Window Server 2003	IIS 6.0
Server3	打印服务器	HP TC4100	Window Server 2003	—

续表

服务器编号	服务器名称	硬件平台	操 作 系 统	服 务 软 件
Server4	数据库服务器	HP TC4100	Window Server 2003	SQL Server
Server5	目录、DNS 服务器	HP TC4100	Window Server 2003	Active Directory
Server6	文件服务器	HP TC4100	Window Server 2003	
Server7	代理服务器	HP TC4100	Window Server 2003	
Server8	邮件服务器	HP TC4100	Window Server 2003	

8.5.5 系统测试

当校园网初具规模后，还应该对校园网的整体运行情况做一下细致的测试和评估。主要的测试内容应该包括：

- 对管理 IP 地址的测试。
- 对相同 VLAN 内的通信进行测试。
- 对不同 VLAN 内的通信进行测试。
- 对冗余链路的工作状态进行测试。
- 对广域网接入路由器上的 NAT 进行测试。
- 对广域网接入路由器上的 ACL 进行测试。
- 对远程访问服务进行测试。
- 对各种服务器提供的服务进行测试。

至于具体的测试步骤，限于篇幅，不再赘述。这里只给出相关测试、诊断命令以供参考。

1. 通用测试、诊断命令

(1) ping ×.×.×.×为标准 ping 命令，用于测试设备间的物理连通性。

(2) 扩展 ping 命令，也用于测试设备间的物理连通性。扩展 ping 命令还支持灵活定义 ping 参数，如 ping 数据包的大小，发送包的个数，等待响应数据包的超时时间等。

(3) traceroute ×.×.×.×命令用于跟踪、显示路由信息。

(4) show running-config 命令用于显示路由器、交换机运行配置文件的内容。

(5) show startup-config 命令用于显示路由器、交换机启动配置文件的内容。

(6) show sessions 命令用于显示从当前设备发出的所有呼出 Telnet 会话。

(7) disconnect 命令用于断开与远程目标主机的 Telnet 会话。

(8) show users 命令用于查看呼入 Telnet 的会话情况。

(9) clear line 命令用于断开远程主机的呼入 Telnet 连接。

(10) shutdown 命令用于临时将某个接口关闭。

(11) no shutdown 命令用于手动启动(激活)处于管理性关闭的接口。

(12) show arp 命令用于显示 ARP 缓存(ARP 表)的内容。

(13) show ip arp 命令用于显示 IP ARP 缓存(ARP 表)的内容。

(14) show interfaces 命令用于显示各接口的状态及参数信息。

(15) show ip interface 命令用于显示 IP 接口的状态及配置信息。

(16) show version 命令用于显示路由器硬件配置、软件版本等信息。

(17) Ctrl＋Shift＋6＋X。该命令也被称为"退出序列",用于终止正在执行的某条命令或操作,也用于从呼出 Telnet 会话中暂时切换到本地连接。

(18) dir flash 命令用于显示闪存中的文件清单。

(19) dir nvram 命令用于显示非易失性内存中的文件清单。

(20) show debugging 命令用于显示正在进行的诊断过程清单。

(21) undebug all 命令用于停止所有诊断过程。

2. 路由和路由协议测试、诊断命令

(1) show ip route 命令用于显示当前路由表内容。

(2) show ip protocols 命令用于显示动态路由协议的配置参数信息。

3. VLAN、VTP 测试、诊断命令

(1) show interface vlan vlan-num 命令用于显示 VLAN 是否已激活、交换机 MAC 基地址、接口参数等。

(2) show mac-address-table 命令用于显示 CAM,即桥接表的内容。该命令可列出学习到的主机 MAC 地址及其所属 VLAN、所处端口、条目类型(静态 STATIC、动态 DYNAMIC 等)以及满足列表条件的 MAC 地址数目。

(3) show vlan 命令用于查看 VLAN 创建情况。该命令可以显示系统所有的 VLAN 信息,包括 VLAN 编号、VLAN 名称、VLAN 状态、VLAN 成员等信息。

(4) show vtp status 命令用于检查 VTP 配置情况。

4. NAT 测试、诊断命令

(1) show ip nat translation 命令用于显示当前正在进行的 NAT 情况。

(2) show ip nat translation verbose 命令用于显示当前正在进行的 NAT 更为详细的情况。

(3) show ip nat statistics 命令用于显示 NAT 运行情况统计。

(4) debug ip nat 命令用于打开对 NAT 的诊断。

5. ACL 测试、诊断命令

(1) show access-lists 命令用于显示所有已定义的访问控制列表内容及命中情况。

(2) show ip access-lists 命令用于显示所有已定义的 IP 访问控制列表内容及命中情况。

6. 远程访问测试、诊断命令

(1) show line 命令用于查看当前系统所有的线路及其状态。

(2) show modemcap 命令用于显示当前路由器可以自动配置的 Modem 列表。

(3) debug ppp negotiation 命令用于打开对 PPP 协议参数协商的诊断。

(4) debug ppp authentication 命令用于打开对 PPP 身份认证过程的诊断。

习　题　8

1. 选择题

(1) 通常认为,决定局域网特性的主要技术有三个,它们是(　　)。

A. 传输媒体、差错检测方法和网络操作系统

B. 通信方式、同步方式和拓扑结构

C. 传输媒体、拓扑结构和媒体访问控制方式

D. 数据编码技术、媒体访问控制方法和数据交换技术

(2) 下列不属于网络设计的基本原则的是(　　)。

A. 可靠性和高性能

B. 可扩展性和可升级性

C. 实用性和经济性

D. 简单性和稳固性

2. 填空题

(1) 大型网络通常采用业界通用的“________—________—________”层次化网络设计模型。

(2) 汇聚层通常为________与________实现基于策略的网络间的连接。

3. 简答题

(1) 简述划分 VLAN 的主要方法。

(2) 什么是模块化设计？有什么好处？

参 考 文 献

[1] [美]Andrew S. Tanenbaum. 计算机网络(第四版). 潘爱民译. 北京：清华大学出版社，2004.
[2] 李越. 计算机网络教程. 北京：清华大学出版社，2006.
[3] 黎元春. 最新 Windows Server 2003 使用指南. 北京：中国科学出版社，2003.
[4] 武文义. Windows Server 2003 计算机网络教程. 北京：北京大学出版社，2003.
[5] 杨尚森. 网络管理与维护技术. 北京：高等教育出版社，2004.
[6] 刘晓平. 校园网综合布线实践. 中国教育网络，2006 年 08 期.
[7] 陈晴. 网络综合布线实用教程. 北京：中国地质大学出版社，2004.
[8] 张文炳. 综合布线技术与实训. 北京：研究出版社，2008.
[9] 高传善. 数据通信与计算机网络(第 2 版). 北京：高等教育出版社，2005.
[10] 蔡皖东. 网络与信息安全. 西安：西北工业大学出版社，2004.
[11] 欧阳江林. 计算机网络实训教程. 北京：电子工业出版社，2004.
[12] 刘四清，田力. 计算机网络实用教程——技术基础与实践. 北京：清华大学出版社，2005.
[13] 周昕. 数据通信与网络技术. 北京：清华大学出版社，2004.